Aug 10th, 12:00 AM

Cyber Risk Assessment and Mitigation Using Logit and Probit Models for DDoS attacks

Kalpit Sharma
Indian Institute of Management Lucknow, fpm18012@iiml.ac.in

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow, arunabha@iiml.ac.in

Cyber Risk Assessment and Mitigation Using Logit and Probit Models for DDoS attacks

Completed Research

Kalpit Sharma
IIM Lucknow
kalpit@iiml.ac.in

Arunabha Mukhopadhyay
IIM Lucknow
arunabha@iiml.ac.in

Abstract

Hackers have been employing Distributed Denial of Service (DDoS) attacks at an unprecedented rate in recent times. In 2018, a 37% rise in such DDoS attacks, wherein traffic reached a peak size of 300 Gbps per attack was alarming. DDoS attacks hinder a business by preventing legitimate customers from accessing the firm's cyber resources (e.g. website, cloud services, streaming quality, etc.). In this study, we aim to assess and mitigate cyber-risk by computing the probability of such DDoS attacks occurring and expected losses associated with them. We use logit and probit models along with standard distribution fitting methods to ascertain the aforesaid questions. Subsequently, we also suggest ways to mitigate cyber-risk resulting due to DDoS attacks by accepting, reducing or passing it. Our study aims to aid CTOs in deciding the best strategy to handle cyber-risk due to DDoS attacks.

Keywords

DDoS, Protection Motivation theory, Rational choice theory, Logit Model, Probit Model, Cyber-risk.

Introduction

Malicious hackers execute Distributed Denial of Service (DDoS) attacks to hinder business globally, by preventing legitimate users from using cyber-resources of the firm. In 2018, the financial losses due to a DDoS attack ranged from US$ 120K to US$ 2M, including direct and indirect losses. In 2018, DDoS attacks were 37% larger in size than the previous year. DDoS attacks inundate the network with data packets as large as 26.37 Gbps on average to overwhelm the network infrastructure (Abrams 2018). Usually, these attackers employ a stealthy web of botnets, which carry out the DDoS attack. Thus, it is difficult to detect the attacker and prevent the attacks in future.

Industries like gaming, video streaming, banking and financial sector (BFSI) which operate on real-time networks suffered from losses amounting to US$ 4 million in 2015 (Sharma and Mukhopadhyay 2020a; Zumberge 2015). The losses have increased astronomically since. In 2019, an unnamed streaming application company was targeted by a DDoS attack for two weeks peaking at 292,000 requests per second, originating from 402,000 different IP addresses (Shani 2019). It resulted in a huge loss of about US$ 200 million for the firm at the rate of US$ 0.5 million peak loss per hour (Bezsonoff 2017). As early as in 2016, the entertainment industry suffered huge losses due to infamous 2016 Dyn server attack; crippled a large number of big digital firms like Netflix, Spotify, Twitter, BBC, CNN, The New York Times, and other entertainment services like HBO Now and Elder Scrolls (Chiel 2017).

The entertainment industry (video streaming, music streaming, gaming, etc.) have been hit by DDoS attacks the worst. Gamers form a lucrative high-spending niche segment who have a tight-knit network with other online game players. Hackers attack multiple nodes by infecting a vulnerable network of gamers and slowly spread the DDoS botnets to other user nodes. Many hackers tend to target popular games to get hold of accounts while they are being used in real-time. Hackers can hide their trail by behaving as gamers and exchanging their loot for in-game items or virtual currency (McKeay 2017). Firms lose approximately US$ 50,000 per hour when under a DDoS attack (Bezsonoff 2017; Sharma and Mukhopadhyay 2020b).

In 2014, the hacker group, *Lizard Squad* took down Sony's PlayStation Network and Microsoft's Xbox Live during Christmas week (Smith 2014). The group; claimed to be launching the attack "for laughs" but

continued causing damage to educate the two giants about strengthening their cyber-security. They chose Christmas as they wanted to harm many users owing to peak transaction volume. In 2019, 51% of the network DDoS attacks lasted less than 15 minutes but many attacks persistently attacked the same target (Avital et al. 2020).

Thus, we intend to estimate the probability of detecting such a DDoS attack and expected loss associated with the same. Subsequently, we intend to map different classes and suggest ways to lower the risk as well as loss severity for ones with extremely high risk and severity.

Literature Review

Cyber risk assessment has been at the helm of cybersecurity research since the advent of Newer Information Technology for businesses (Gordon et al. 2003). Assessment of risk helps identify and subsequently quantify the probability of a cybersecurity incident occurring provided the security protocols were in place. The cyber risk assessment also aids in evaluating the efficacy of IT risk management compliance structure already in place in organizations.

Cyber risk assessment methods intend to identify information assets (such as hardware, systems, laptops, customer data, and intellectual property) which can be under cyber-attack and their associated risks. Information assets are divided into multiple classes according to the perceived risk in order of their severity, and broken into sub-parts to correctly identify the risky component of the asset and its type (tangible, intangible, etc.) (O'Reilly et al. 2018). The risk assessment stage is followed by quantification of identified risk with the help of diverse methods aiming at attaching a monetary value to it.

Cyber risk quantification methods rely on the probability of a risky incident occurring and rigorous estimation of loss amount for such incidents. Thus, the accuracy of such methods relies on the accuracy of risk identification as well as loss calculation. Loss estimation methods also evolve according to the unit of analysis and definition of loss for which we are undertaking the aforesaid exercise. Thus, the expected loss for entity resulting due to cyberattacks depends not only on the incident but also on our ability to accurately estimate its loss. These estimations also vary in their methodological rigor depending upon the type and granularity of data available to calculate them. Cyber risk quantification techniques range from mathematical risk modelling to data mining methods using empirical data available from security providers (Campbell and Stamp 2004).

Many of the initial quantitative approaches tried to model the cyber risk scenario as an uncertainty model where the probability of cyber risk occurrence is to be studied. Most of these classification model use traffic attributes such as TCP/IP layer used for the attack, quanta of bits used and packet structure to typify cyber-attacks' presence or otherwise. The uncertainty of classification can be modelled using various statistical methods which use some prior knowledge of the occurrence of a cyber breach and update it with current evidence through data. Logit and probit models have been used to calculate the probability of a cyber risk occurring using CSI-FBI survey data from 1997-2010 (Mukhopadhyay et al. 2019). Machine learning techniques such as Bagger classifier and CART based hybrid classifier are efficient at assessing phishing attacks (Biswas and Mukhopadhyay 2017). On the other hand, augmented decision tree classifier along with Chi-square and Symmetric uncertainty were found to be effective in analysing DDoS feature vectors from CAIDA dataset (Balkanli et al. 2015). Copula-based methods, that are quite popular with actuarial researchers, quantified cyber risk and thus, were used to propose insurance approaches in complex risk modelling situations such as cyber-attacks (Herath and Herath 2011). It has been previously shown that cyber risk attack vectors can be efficiently modelled using density estimation methods and thus, augment the accuracy of a method that relies upon distribution statistics to classify (Alhazmi et al. 2007). Fuzzy logic-based RiMaHCoF method was able to quantify cyber-risks in overlapping and conflicting risk classes (Smith and Eloff 2002).

Decision trees and their other variants like ensemble methods, hybrid classifiers are quite efficient with provision for decision rules for informing future decisions for classifying similar incident vectors. The use of only a small number of independent features constructs a very highly complex tree and pruning it becomes difficult given the trade-off with its accuracy (Biswas et al. 2016). Thus, a large stress is on finding interpretable quantitative method to ascertain probability of a cyber-attack occurring.

Theoretical Foundation

We model our study on basis of protection responses of firms when they are motivated to do so under a fear appeal. Protection-motivation theory states that the magnitude of fear appeal, probability of that event occurring and efficacy of response are the chief descriptors of firms' behavior under an cyber-attack (Boss et al. 2015; Rogers 1975). Firm also evaluate risks by weighing the costs and benefits to select the best outcome in such a situation. Rational-choice theory states that choice of outcome is subjective and depends on the preference structure of the decision maker, that is, firms in this case (Becker 1978; Kahneman and Tversky 1979a). The costs and benefits of the intended responses or outcomes can be constrained in terms of time, money or effort. Some protection responses demand to be implemented quickly otherwise their efficacy suffer drastically.

Similarly, cyber-criminals also weigh in their options while executing the attack and thus, the most lucrative firms in terms of money and vulnerability are usually targeted. Criminals are also constrained in terms of effort, time and money. They must execute least possible attacks and cause more harm at the same time to the targets. Thus, they usually target firms with high number of vulnerabilities exposed and moderate to high customer base.

Firms choose between different alternatives of hedging their cyber-risks by selecting options with least monetary loss and quality of service. This is in line with the prospect theory which states that firms and individuals works on loss aversion and carefully evaluates their risks and benefits before making real-life choices (Kahneman and Tversky 1979b).

Proposed Model

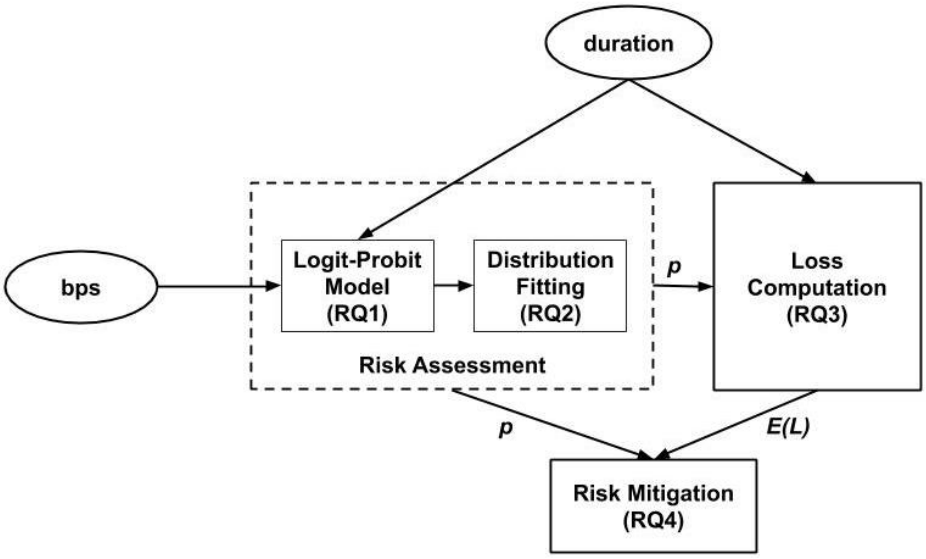

Figure 1: CRAM-D Research Model

Figure 1 depicts the proposed Cyber-risk Assessment and Mitigation model for DDoS (CRAM-D) which consists of three modules namely Risk Assessment, Loss Computation and Risk Mitigation. The model takes attack vector features, that is, *bits per second (bps)* and *duration* of the DDoS attack and outputs possible risk mitigation strategies by estimating probability of attack and subsequent expected loss in intermediate steps. Through CRAM-D model, we intend to investigate following research questions under aforementioned modules.

- RQ1: What is the probability (p) of a DDoS attack on a business organization given the intensity and duration of the DDoS attack?

- RQ2: What is the best statistical approximation of probability of an DDoS attack and loss occurring due to it?
- RQ3: What is the expected loss (*E(L)*) from a DDoS attack on an organization?
- RQ4: What risk mitigation strategy can CTOs choose for each type of DDoS attack?

Data

In this study, we have used a dataset of DDoS attacks occurring in the online gaming industry that were recorded by Akamai's Prolexic software solution. The dataset consists of 10329 records from 2012 to 2018. Each record consists of three attack-specific variables namely *bits per second (bps)* received during the attack, *packets per second (pps)* received during the attack and the *start* and *end timestamp* of the attack. We have calculated the *duration* of attack as a new variable by using *start* and *end timestamp* attributes. We also have the *types* attributes that indicates the variant of DDoS attack that has occurred for that record. It also informs us whether the DDoS attack is a mixture of two or more attacks. The attribute bps and pps are highly correlated and thus, we drop pps from our final feature vector. bps attribute has been converted to Gigabits per second to match the scale of other variables. Duration has also been converted to hours for the aforesaid reason. Table 1 provides summary statistics of the aforesaid attributes.

To pre-process our data according to our methodology, we arrange data records according to year and month of occurrence of that DDoS attack. Thus, for each month of the year, we have total number of DDoS attacks occurring and its breakdown in the six specific types of DDoS attack as mentioned in Table 2. For each month, we also have average intensity of attack (in Gbps) and average duration (in hours) of attacks of each type. These derived attributes will aid in designing a model to predict the probability of occurrence of each type of attack.

Table 1: Descriptive Statistics for the dataset (N=10,329)

Variable	Count	Mean	Standard Deviation	Minimum	Maximum
pps	10329	323639	52947	0	5887744
bps (in Gb per second)	10329	1.62	2.66	0	27.88
Duration (in hours)	10329	19.7	14.2	0.03	69.43

Table 2: Attack Composition

Attack Class	Attack type	Number of records
A	DNS Flood (DF), UDP Fragment (UFR)	3155
B	NTP Flood (NF)	2671
C	CharGEN Attack (CGA), UDP Fragment (UFR)	2030
D	SSDP Flood (SF)	1465
E	UDP Flood (UFL)	1008

Methodology

Risk Assessment

In this study, we have used logit-probit models (eq 1,2) to predict the probability (p) of each type of DDoS attack occurring based on intensity of attack (i.e. Gbps of attack) and duration of the attack (Mukhopadhyay et al. 2019). We have taken the training set of attacks that occurred from 2012 to 2016 and testing set from 2017 to 2018. The ratio of training set to testing set is roughly 80:20.

$$Logit\ Model: \quad E(Y \mid X = bps, duration) = p = \frac{1}{1 + e^{-(\beta_0 + \beta_1 bps + \beta_2 duration)}} \tag{1}$$

$$Probit\ Model: \quad E(Y \mid X = bps, duration) = p = \Phi^{-1}(\beta_0 + \beta_1 bps + \beta_2 duration) \tag{2}$$

Next, we try to generalize the probability of aforesaid DDoS attacks by fitting a beta distribution (eq.3) on the probability values thus generated for each type of attack. The aforesaid distribution fitting gives us central tendency measures such as mean for probability values which will be used while informing our risk mitigation strategies.

$$Prob(p) = \frac{(1-p)^{b-1}p^{a-1}}{B(a,b)}, \text{where } B(a,b) \text{is the beta function and p is the probability of attack.} \quad (3)$$

Loss Computation

In this module, we calculate total loss for each data record at the rate of US$ 0.5 million per hour (Bezsonoff 2017; Sharma and Mukhopadhyay 2020b). We generalize the loss in each attack type as a gamma distribution (eq.4) and similarly, calculate mean loss amount for each type of DDoS attack. Next, we calculate expected loss for each attack type.

$$Prob(L) = \frac{L^{\alpha-1}e^{-L/\lambda}}{\Gamma(\alpha)\lambda^{\alpha}}, \text{where } \Gamma(\alpha) \text{ is the gamma function and L is the loss amount for that attack type.} \quad (4)$$

Risk Mitigation

We plot the expected loss and probability of attack types on a heat matrix to tag attack types according to levels of criticality. If the probability of occurrence for an attack is less than 0.5 then it is low risk quadrant otherwise high. If the expected loss is less than US$ 1.78 million then the attack type falls in low severity quadrant otherwise high. The boundary values dividing the quadrants are chosen by the CTO and strategies decided in accordance with firm's security attitude. Thus, the heat mastrix is divided into 4 quadrants with varying combinations risk-severity values.

Results and Discussion

Risk Assessment

We assess risk by calculating probability of DDoS attack using logit and probit models. Table 3 details the coefficients for each type of DDoS attack in both the modelling exercises (eq. 1 and 2).

Table 3: Coefficients of Logit and Probit model for training set (from 2012 to 2016)

	Logit Model					Probit Model				
	coeff	SE	t	p	dev	coeff	SE	t	p	dev
CGA	-1.990	0.235	-8.484	0.000	159.863	-1.173	0.135	-8.673	0.000	158.755
	0.487	0.070	6.931	0.000		0.293	0.042	7.040	0.000	
	0.009	0.010	0.932	0.351		0.004	0.006	0.689	0.491	
DF	-0.697	0.194	-3.585	0.000	227.381	-0.448	0.116	-3.852	0.000	227.479
	-0.119	0.022	-5.305	0.000		-0.070	0.013	-5.297	0.000	
	0.006	0.009	0.660	0.510		0.004	0.006	0.765	0.444	
NF	-1.513	0.294	-5.140	0.000	102.663	-0.916	0.174	-5.275	0.000	102.658
	-0.065	0.027	-2.381	0.017		-0.038	0.016	-2.393	0.000	
	0.031	0.013	2.388	0.017		0.018	0.008	2.377	0.444	

Figure 2 illustrates fitted data points (in red) along with actual data points (in blue) where y-axis denotes the proportion or probability of occurrence for each attack points in the dataset.

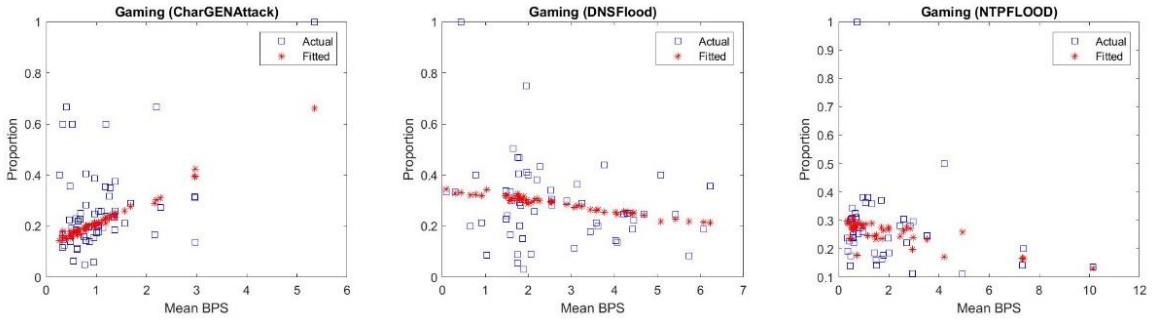

Figure 2: Fitted Logit Model Vs Actual Data Points for each attack type

Next, we fit a beta distribution to the probability values given by logit model in the last step. Table 4 details the generated parameters of beta distribution, a and b along with mean and standard deviation of the fitted distribution (eq. 3). Figure 3 depicts the fitted beta distribution curve for each DDoS attack type.

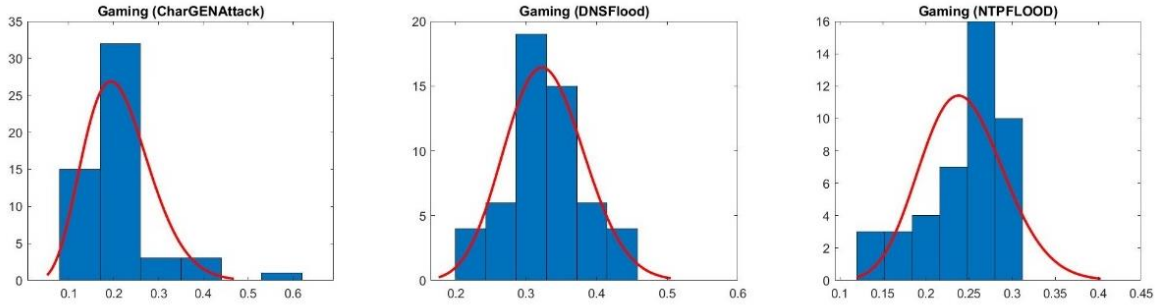

Figure 3: Fitted Beta distribution curve for probability of DDoS attacks of each type

Table 4: Parameter estimates of beta distribution for probability of each DDoS attack type

Attack type	a	b	Mean	Standard Deviation
CGA	6.62	24.36	0.21	0.07
DF	22.73	46.63	0.32	0.05
NF	19.35	59.80	0.24	0.04

Loss Computation

Figure 4 illustrates the curve fitting exercise undertaken to ascertain suitability of gamma distribution for approximating losses due to cyber-risks (Mukhopadhyay et al. 2007). Table 5 tabulates parameters of gamma distribution α and λ along with mean and standard deviation loss amount for each attack type. Table 6 records the probability of each attack type and expected loss for the firm because of the DDoS attack.

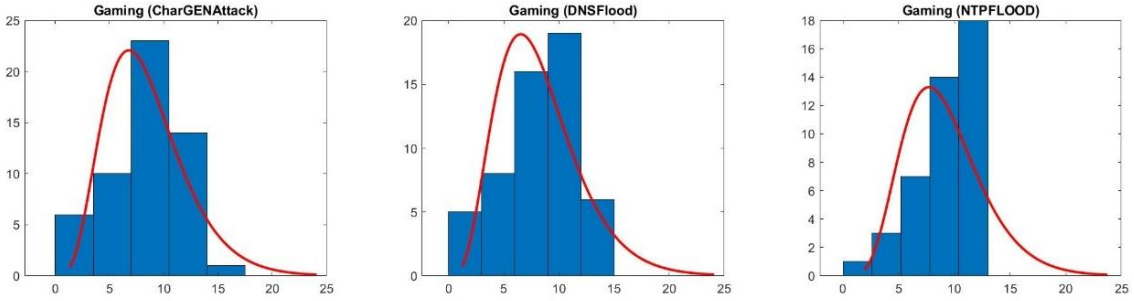

Figure 4: Fitted Gamma distribution curve for loss occurring in each attack type

Table 5: Parameter estimates of gamma distribution for loss occurring in each DDoS attack type

Attack type	α	λ	Mean	Standard Deviation
CGA	5.10	1.65	3.08	1.36
DF	4.81	1.71	2.81	1.28
NF	6.43	1.41	4.54	1.79

Table 6: Risk and Severity Matrix

Attack type	Risk: Probability of DDoS attack (p)	Severity: Expected loss (in millions of US$) $E(L) = p * L$
CGA	0.21	0.65
DF	0.32	0.90
NF	0.24	1.09
SF	0.19	3.56
UFL	0.1	0.18
UFR	0.5	1.89

Risk Mitigation

Figure 5 depicts a heat matrix calculated from the model that situates the different DDoS attacks in terms of Risk × Severity. This helps a chief technology officer (CTO) to prioritize the risk mitigation strategy, such as technological intervention to reduce the risk or transfer risk through cyber-insurance. For example, a DDoS attack of type UFR is in the high risk-high severity quadrant, while attacks NF, DF, CGA, and UFL are in the low risk-low severity quadrant. Therefore, the Chief Technology Officer (CTO) of an enterprise at risk of DDoS attacks of type UFR should consider implementing the following risk mitigation strategies: First, add stringent firewalls or intrusion detection systems or divert excess/illegitimate traffic to backup servers/content delivery networks (CDNs) to reduce the risk and thus lower the severity of DDoS attack. Next, transfer the residual risk by subscribing to cyber-insurance policies, thus moving into the low risk-low severity quadrant (Biswas et al. 2017; Das et al. 2019; Kunreuther 1997).

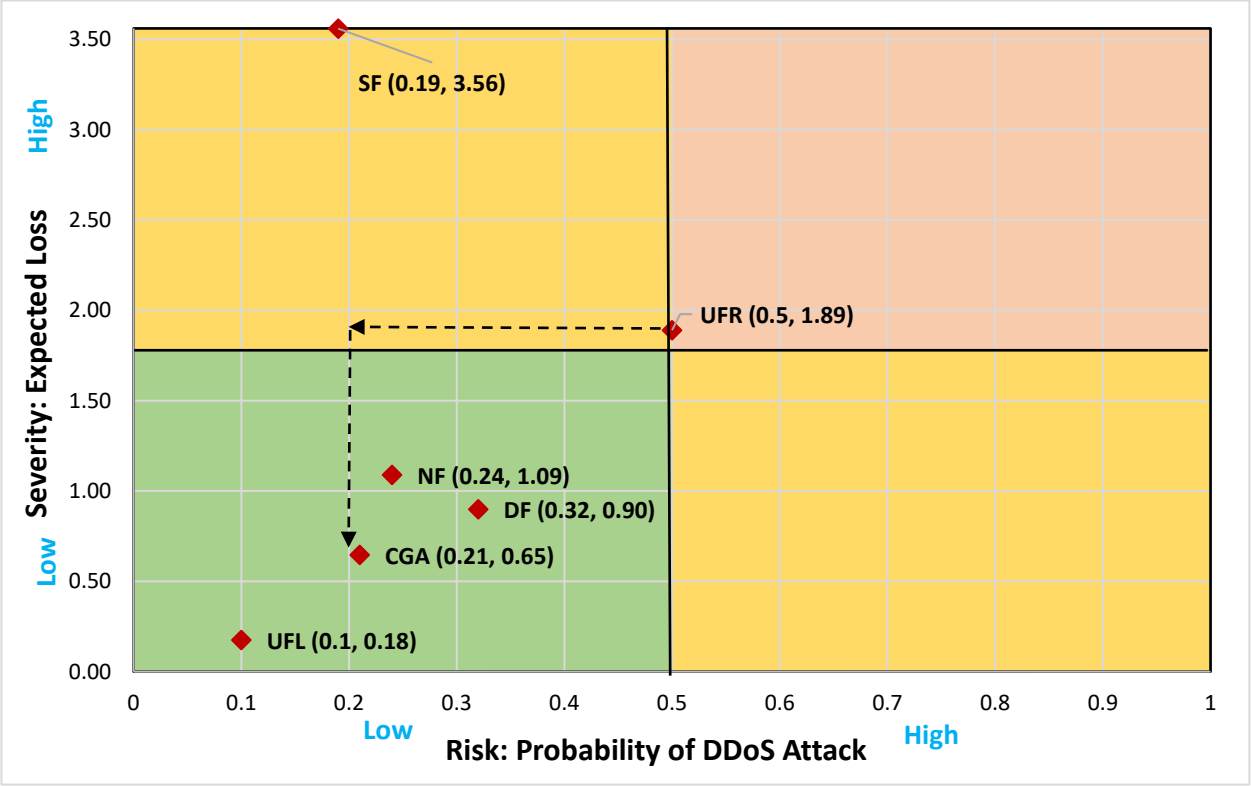

Figure 5: Risk Mitigation Heat Matrix

The predictions made in this study are based on historical data, and thus we assume that attackers behave a certain way. It is very likely that the pattern of attacks will change in response to firms' defenses to it. The generalizability of the study is limited to online gaming industry. The future research will aim at comparing risk mitigation strategies across different industries and temporal analysis of DDoS attacks. Prior security investments and DDoS attack vectors can also be studied as antecedents to future attack intensity and duration.

Conclusion

Our study helps in predicting the probability of DDoS attacks of aforesaid six types occurring in the gaming industry. It also helps in quantifying expected loss for each attack type. It helps the CTO in taking informed decisions while drafting the security mechanisms according to the risk profile of the firm. It also helps them decide whether to accept the cyber-risk or reduce it. If possible, they can pass or avoid the cyber-risk by using appropriate technological interventions combined with cyber-insurance.

References

Abrams, L. 2018. "Dramatic Increase of DDoS Attack Sizes Attributed to IoT Devices," *Bleeping Computer*, BleepingComputer.com, September. (https://www.bleepingcomputer.com/news/security/dramatic-increase-of-ddos-attack-sizes-attributed-to-iot-devices/).

Alhazmi, O. H., Malaiya, Y. K., and Ray, I. 2007. "Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems," *Computers and Security* (26:3), pp. 219–228. (https://doi.org/10.1016/j.cose.2006.10.002).

Avital, N., Zawoznik, A., Azaria, J., and Lambert, K. 2020. "2019 Global DDoS Threat Landscape Report: Imperva," *Imperva Blog*, Imperva, February. (https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/).

Balkanli, E., Nur Zincir-Heywood, A., and Heywood, M. I. 2015. "Feature Selection for Robust Backscatter DDoS Detection," in *Proceedings - Conference on Local Computer Networks, LCN* (Vol. 2015-Decem), IEEE, October, pp. 611–618. (https://doi.org/10.1109/LCNW.2015.7365905).

Becker, G. S. 1978. *The Economic Approach to Human Behaviour*, The University of Chicago Press. (https://www.ebook.de/de/product/3626539/gary_s_becker_the_economic_approach_to_human_behaviour.html).

Bezsonoff, N. 2017. "The State of DDoS Attacks in 2017: Neustar Blog," *The State of DDoS Attacks in 2017 | Neustar Blog*, Neustar, October. (https://www.home.neustar/blog/neustar-global-attacks-and-cyber-security-insight-report).

Biswas, B., and Mukhopadhyay, A. 2017. "Phishing Detection and Loss Computation Hybrid Model: A Machine-Learning Approach," *ISACA Journal* (1), pp. 22–29.

Biswas, B., Mukhopadhyay, A., and Dhillon, G. 2017. "GARCH-Based Risk Assessment and Mean-Variance-Based Risk Mitigation Framework for Software Vulnerabilities," in *AMCIS 2017: A Tradition of Innovation - 23rd Americas Conference on Information Systems*.

Biswas, B., Pal, S., and Mukhopadhyay, A. 2016. "AVICS-Eco Framework: An Approach to Attack Prediction and Vulnerability Assessment in a Cyber Ecosystem," in *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly: Management Information Systems* (39:4), pp. 837–864. (https://doi.org/10.25300/MISQ/2015/39.4.5).

Campbell, P. L., and Stamp, J. E. 2004. "A Classification Scheme for Risk Assessment Methods."

Chiel, E. 2017. "Here Are the Sites You Can't Access Because Someone Took the Internet Down," *Splinter News*, , July. (https://splinternews.com/here-are-the-sites-you-cant-access-because-someone-took-1793863079).

Das, S., Mukhopadhyay, A., Saha, D., and Sadhukhan, S. 2019. "A Markov-Based Model for Information

Security Risk Assessment in Healthcare MANETs," *Information Systems Frontiers* (21:5), pp. 959–977. (https://doi.org/10.1007/s10796-017-9809-4).

Gordon, L. A., Loeb, M. P., and Sohail, T. 2003. "A Framework for Using Insurance for Cyber-Risk Management," *Communications of the ACM* (46:3), ACM, pp. 81–85. (https://doi.org/10.1145/636772.636774).

Herath, H. S. B., and Herath, T. C. 2011. "Copula-Based Actuarial Model for Pricing Cyber-Insurance Policies," *Workshop on the Economics of Information Security* (2:1), pp. 7–20. (http://weis2007.econinfosec.org/papers/24.pdf).

Kahneman, D., and Tversky, A. 1979a. "An Analysis of Decision under Risk," *Econometrica*.

Kahneman, D., and Tversky, A. 1979b. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* (47:2), pp. 263–291. (https://doi.org/10.2307/1914185).

Kunreuther, H. 1997. "Managing Catastrophic Risks through Insurance and Mitigation," *Philadelphia, Wharton Risk Management and Decision Processes Center*, pp. 1–31. (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.41.6268&rep=rep1&type=pdf).

McKeay, M. 2017. "Q4 2017 State of the Internet Security Report," *Akamai Technologies*. (https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf).

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., and Shukla, G. K. 2019. "Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance," *Information Systems Frontiers* (21:5), pp. 997–1018. (https://doi.org/10.1007/s10796-017-9808-5).

Mukhopadhyay, A., Chatterjee, S., Roy, R., Saha, D., Mahanti, A., and Sadhukhan, S. K. 2007. "Insuring Big Losses Due to Security Breaches through Insurance: A Business Model," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, IEEE, pp. 158a-158a. (https://doi.org/10.1109/HICSS.2007.280).

O'Reilly, P. D., Rigopoulos, K., Witte, G., and Feldman, L. 2018. "2017 Annual Report: NIST/ITL Cybersecurity Program," Gaithersburg, MD, September. (https://doi.org/10.6028/NIST.SP.800-203).

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91:1), pp. 93–114. (https://doi.org/10.1080/00223980.1975.9915803).

Shani, T. 2019. "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important.: Imperva," *Imperva*, , June. (https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/).

Sharma, K., and Mukhopadhyay, A. 2020a. "Cyber Risk Assessment and Mitigation Strategy for DDoS Attacks in BFSI Segment," in *19th Annual Security Conference*, Las Vegas, NV.

Sharma, K., and Mukhopadhyay, A. 2020b. "Assessing the Risk of Cyberattacks in the Online Gaming Industry: A Data Mining Approach," *ISACA Journal* (2).

Smith, D. 2014. "Why Hacker Gang 'Lizard Squad' Took Down Xbox Live And PlayStation Network," *Business Insider*, , December. (http://www.businessinsider.com/why-hacker-gang-lizard-squad-took-down-xbox-live-and-playstation-network-2014-12).

Smith, E., and Eloff, J. H. P. 2002. "A Prototype for Assessing Information Technology Risks in Health Care," *Computers & Security* (21:3), pp. 266–284. (https://doi.org/10.1016/s0167-4048(02)00313-9).

Zumberge, M. 2015. "Cyber Attacks on the Rise in Media Biz Since Sony Hack: Survey (Exclusive)," *Variety*, Penske Media Corporation, November. (https://variety.com/2015/digital/news/sony-hack-anniversary-cybersecurity-data-1201633671/).