Aug 10th, 12:00 AM

Cyber-risk assessment and mitigation of DDoS attacks using semi-structured data models

Kalpit Sharma
Indian Institute of Management Amritsar, kalpits@iimamritsar.ac.in

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

Cyber-risk assessment and mitigation of DDoS attacks using semi-structured data models

Emergent Research Forum (ERF)

Kalpit Sharma
Indian Institute of Management
Amritsar
kalpits@iimamritsar.ac.in

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

Abstract

This study attempts to mitigate DoS attacks by combining structured and unstructured data. It comprises three modules. Specifically, our cyber-risk assessment module uses input such as DDoS attack characteristics: attack intensity and duration; Massively Multiplayer Online Gaming (MMOG) platform characteristics: vulnerability counts, severity, trends, and effect of cybersecurity spending, along with web articles. Following this, we calculate the expected loss resulting from a DDoS attack on a gaming company. We conclude by suggesting cyber-risk mitigation strategies such as self-protection (technology, compliance, and legal deterrence), self-insurance, or cyber-insurance.

Keywords

Cyber-risk, DDoS, Semi-structured data, cyber-insurance

Introduction

Recently, cyber-risk has become one of the most pervasive risks facing the global community. The World Economic Forum (WEF) has listed cybersecurity failure as one of the top five global risks since 2018 (McLennan 2021). According to the WEF survey of 2020, 39 percent of respondents identified cyber-risk as a highly likely and high impact risk for industries, governments, and individuals (McLennan 2021). This study investigates three main research questions. Firstly, we estimate the probability of DDoS attacks using attack, platform traits, and news articles detailing them. Next, we compute the expected loss incurred during these attacks. Subsequently, we devise mitigation strategies for Chief Technology Officers (CTOs) to accept, reduce, or pass the cyber-risk using a hybrid solution comprising technological and financial means such as cyber-insurance.

Proposed Model

Using the opportunity theory of crime, apart from the initial stimulus, the hacker looks for vulnerabilities in the systems in an environment with few or no checks (Cohen and Felson 1979). Additionally, hackers weigh the benefits of their actions against the costs they face in terms of effort, time, and punishment, if any. They assess the probability of the event occurring and its impact on them. According to rational choice theory, decision-makers opt for the alternative that best matches their subjective preferences (Becker 1978; McCarthy 2002). Cyber-risk management closely follows the principles of risk theory (Kunreuther 1997). Based on the discussion above, we propose the model consisting of three modules: Cyber-risk assessment, Cyber-risk quantification, and Cyber-mitigation for an MMOG firm, as illustrated in Figure 1.

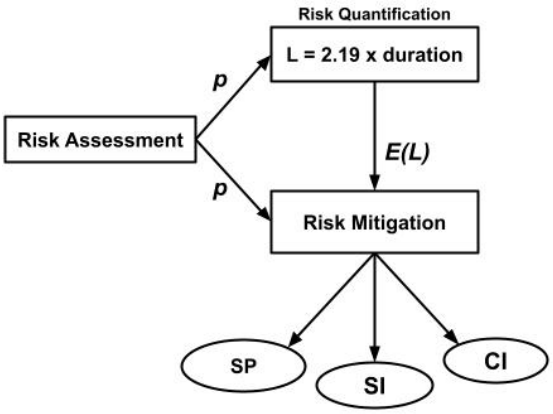
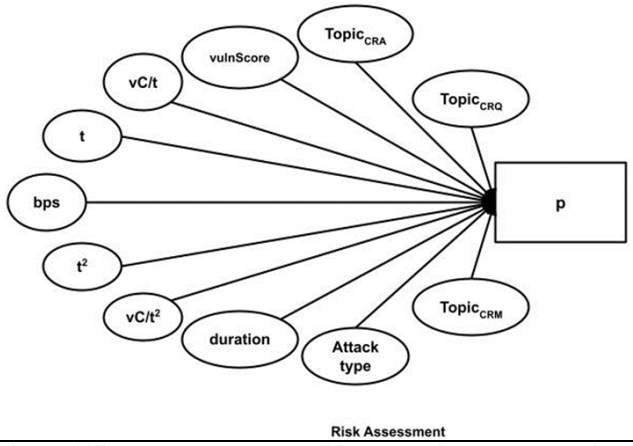


Figure 1: Proposed model



vC = Vulnerability count, t = Time, vulnScore = Vulnerability score, SP = Self-protection, CI = Cyber-insurance, SI = Self-insurance, p = probability, E(L) = Expected Loss, L= Loss

Figure 2: Cyber-risk assessment module for the proposed model

Cyber-risk Assessment

Figure 2 depicts the cyber-risk assessment module. Thus, we investigate,

RQ1: What is the probability of DDoS attacks of each kind?

Logit model:

$$p_{type} = \frac{1}{1 + e^{-Z_i}} \quad (1)$$

$$Z_i = \beta_0 + \beta_1 bps + \beta_2 duration + \beta_3 t + \beta_4 t^2 + \beta_5 vulnScore + \beta_6 \frac{vC}{t} + \beta_7 \frac{vC}{t^2} + \beta_8 Topic_{CRA} + \beta_9 Topic_{CRQ} + \beta_{10} Topic_{CRM}$$

p_{type} = probability of DDoS attack, type = NTPFlood, UDPFlood, SSDPFlood, UC, UD

Cyber-risk Quantification

In the second stage of the proposed model, we calculate the expected loss that indicates the severity of the DDoS attack. We assume that a company loses US$ 2.19 million per hour as a result of a DDoS attack (Mukhopadhyay et al. 2019). Thus, expected loss (Courtney 1977) is the product of the probability of attack with the loss incurred as a result of the attack.

RQ2: What is the expected loss for each type of DDoS attack?

Cyber-risk Mitigation

In the final stage, the proposed model suggests ways to reduce the risk and severity of DDoS attacks in the MMOG industry via cyber-risk mitigation. Risk (Probability of attack) and severity (Expected loss) are the primary inputs for this stage. We can use this information to determine if the CTO of the firm should reduce (self-protection), accept (self-insurance), or transfer (cyber-insurance) risk (Böhme and Kataria 2006).

RQ3: What cyber-risk mitigation strategies should CTOs use for each kind of DDoS?

Methodology

Using the GLM (i.e., logit model)(Pregibon and Hastie 2017), we predict the probability of five types of DDoS attacks in each quarter. Next, we assume that firms lose US$ 2.19 million per hour as a result of DDoS attacks. Subsequently, we compute the expected loss for each data record. We then suggest mitigation strategies by visualizing the risk (probability of the attack) and severity (expected loss as a result of the attack) appropriately. Thus, the firm can select between self-protection, self-insurance, or cyber-insurance.

Data

This study uses data on characteristics of DDoS attacks on MMOG platforms that are obtained from a Content Delivery Network (CDN). In addition, we have analyzed MMOG platform-specific vulnerabilities from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) datasets for each respective quarter. As shown in Table 1, the CDN dataset contains 10,329 records aggregated into 25 quarters (from 2012 Q2 to 2018 Q2). The dataset includes five types of DDoS attacks. We augment the dataset with topic classification related to cyber-risk assessment, quantification, and mitigation extracted through web articles from popular cybersecurity newsgroups for the respective quarters. They are coded as dummy variables for each quarter, with '0' signifying the absence of the same.

	Variables	N	N_{final}	Attack trait	Mean	Std. Dev.	Source
Attack type	UDP Fragment, DNS Flood (UD)	3,155	23	bps (Gbps) duration (hours)	2.7 19.0	3.2 13.8	Reputed CDN
	NTP Flood	2,671	19	bps duration	1.1 20.2	1.8 14.1	
	UDP Fragment, CharGEN Attack (UC)	2,030	20	bps duration	0.9 19.9	1.2 14.1	
	SSDP Flood	1,465	16	bps duration	0.8 20.8	1.3 15.1	
	UDP Flood	1,008	17	bps duration	1.8 19.1	4.1 14.3	
	Topic_CRA	25	25	—	—	—	Web Articles
	Topic_CRQ	25	25	—	—	—	
	Topic_CRM	25	25	—	—	—	
MMOG platform traits	Vulnerability Score	23,712	25	—	6.2	2.0	NVD feeds
	t* (quarters)	25	25	—	—	—	
	t^2* (quarters)	25	25	—	—	—	
	Vulnerability Count	23,712	25	—	—	—	

*Training set = 2012 Q2 to 2017 Q1 (20 quarters), Testing = 2017 Q2 to 2018 Q2, N_{final} = number of quarterly records

Table 1: Summary statistics (2012 Q2 to 2018 Q2)

Table 2 details the correlation matrix of the predictors and target variables in the model.

	p	*bps*	*duration*	*t*	t^2	*vulnSc*	*vC/t*	vC/t^2
p	1							
bps	-0.07	1						
duration	-0.03	0.01	1					
t	-0.56^{***}	-0.20^{**}	0.21^{**}	1				
t^2	-0.41^{***}	-0.24^{**}	0.15	0.98^{***}	1			
vulnSc	0.12	0.29^{***}	0.10	-0.60^{***}	-0.69^{***}	1		
vC/t	0.63^{***}	-0.01	-0.18^{*}	-0.51^{***}	-0.38^{***}	0.08	1	
vC/t^2	0.51^{***}	-0.02	-0.17^{*}	-0.37^{***}	-0.26^{**}	0.08	0.95^{***}	1

*** p<0.01, ** p<0.05, * p<0.1

Table 2: Correlation matrix (N = 95)

Results

This section details the results from the three stages of this study.

Cyber-risk Assessment

Logit and Probit models give the probability of an attack of each type occurring in the future. Table 3 details the coefficients for each type of DDoS attack in both the modeling exercises.

Logit Model (M1)

		Coeff.	SE	t	p	Dev.		Coeff.	SE	t	p	Dev.
	β_0	-41.36	9.97	-4.15	0.00	12	UD	1.11	10.3	0.11	0.91	34
	bps	0.05	0.07	0.77	0.44			0.09	0.13	0.72	0.47	
	dur	0.12	0.06	1.90	0.06			-0.07	0.05	-1.43	0.15	
	t	3.93	1.25	3.13	0.00			-0.19	1.11	-0.17	0.86	
	t^2	-0.11	0.04	-2.95	0.00			0.01	0.03	0.29	0.77	
NF	vulnSc	0.06	0.50	0.12	0.91			-0.12	0.43	-0.27	0.79	
	vC/t	-0.14	0.07	-2.00	0.05			-0.03	0.05	-0.54	0.59	
	vC/t^2	3.44	1.18	2.91	0.00			0.34	0.94	0.37	0.71	
	$Topic_{CRA}$	-0.08	0.16	-0.49	0.62			0.59	0.38	1.57	0.12	
	$Topic_{CRQ}$	1.36	0.50	2.74	0.01			-0.91	0.29	-3.09	0.00	
	$Topic_{CRM}$	-0.34	0.20	-1.69	0.09			0.15	0.37	0.40	0.69	
	β_0	-15.48	11.19	-1.38	0.17	27	UDF	-4.36	7.39	-0.59	0.55	12
	bps	-1.14	0.36	-3.20	0.00			-0.03	0.09	-0.39	0.70	
	dur	-0.24	0.05	-4.52	0.00			-0.08	0.03	-2.23	0.03	
	t	4.23	2.14	1.98	0.05			-0.81	1.37	-0.59	0.55	
	t^2	-0.14	0.07	-2.11	0.03			0.03	0.04	0.83	0.41	
SF	vulnSc	-1.66	0.73	-2.29	0.02			1.04	0.58	1.79	0.07	
	vC/t	-0.13	0.08	-1.69	0.09			-0.03	0.05	-0.61	0.54	
	vC/t^2	2.47	1.20	2.06	0.04			0.37	0.64	0.58	0.56	
	$Topic_{CRA}$	-0.56	0.17	-3.30	0.00			0.45	0.21	2.14	0.03	
	$Topic_{CRQ}$	-1.28	0.28	-4.57	0.00			0.26	0.25	1.03	0.30	
	$Topic_{CRM}$	1.12	0.35	3.15	0.00			0.21	0.29	0.73	0.47	
	β_0	-13.99	4.28	-3.27	0.00	36						
	bps	-0.67	0.28	-2.40	0.02							
	dur	0.01	0.02	0.30	0.76							
	t	3.00	0.78	3.87	0.00							
	t^2	-0.10	0.02	-4.16	0.00							
UC	vulnSc	-1.37	0.29	-4.64	0.00							
	vC/t	-0.08	0.03	-2.82	0.00							
	vC/t^2	1.49	0.43	3.51	0.00							
	$Topic_{CRA}$	-0.05	0.13	-0.37	0.71							
	$Topic_{CRQ}$	-0.58	0.15	-3.74	0.00							
	$Topic_{CRM}$	0.29	0.15	1.93	0.05							

Coeff. =Coefficients, Dev.=deviance, dur=duration, vulnSc. =Vulnerability score, *** p<0.01, **p<0.05, *p<0.1

Table 3: Coefficients of logit and probit models (Training set = 2012 Q2 to 2017 Q1)

Cyber-risk Quantification

Table 4 records the risk and severity (i.e., p * 2.19) values for each DDoS attack (Mukhopadhyay et al. 2019).

Attack type	Risk: Probability of DDoS attack (p)	Severity: Expected loss (in millions USD)
NTPFlood	0.21	0.65
SSDPFlood	0.32	0.90
UC	0.24	1.09
UD	0.19	3.56
UDPFlood	0.1	0.18

Table 4: Risk and Severity Matrix

Cyber-risk Mitigation

Figure 3 displays a heat matrix that illustrates how the different DDoS attacks are calculated as risk and severity ordered pair. For example, a DDoS attack of type UC, UD, and UDPFlood are in the high risk-high severity quadrant, while attacks NTPFlood and SSDPFlood are in the low risk-low severity quadrant. Accordingly, an enterprise at risk of DDoS attacks of the type UFR should consider implementing strict firewalls or intrusion detection systems or divert excess or illegitimate traffic to backup servers or content delivery networks (CDNs) to reduce the risk. As a next step, subscribe to cyber-insurance policies to transition into the low-risk-low severity quadrant (Das et al. 2019; Kunreuther 1997).

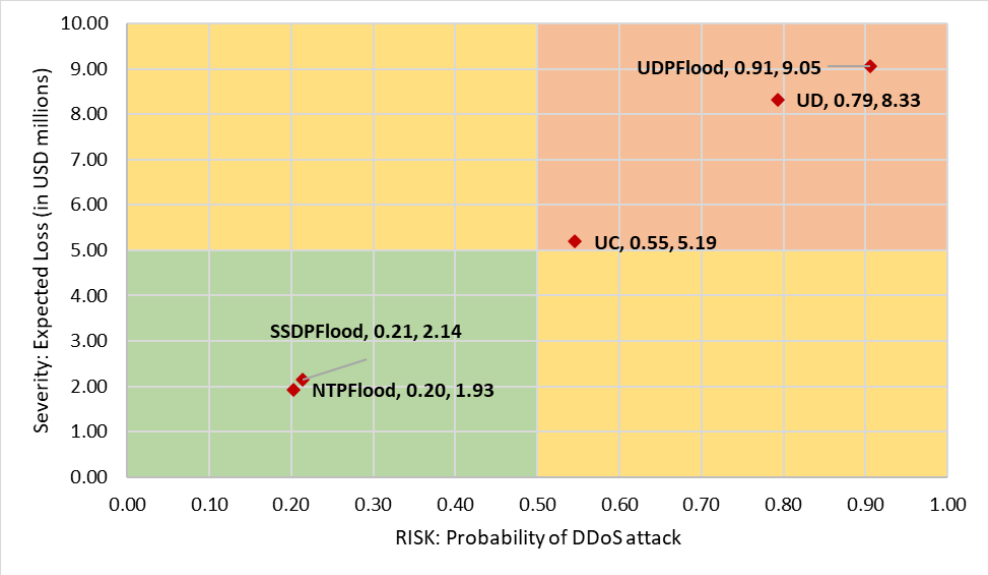


Figure 3: Risk-Severity heat matrix

Conclusion

According to our study, DDoS attacks of the five types of attacks mentioned above are more likely to occur in the gaming industry. The study also assists in quantifying expected losses for each attack type. It helps the CTO make informed decisions when drafting security mechanisms for the risk profiles of the company. As a result, they can determine whether to accept or reduce the cyber-risk. When appropriate technological interventions such as intrusion detection systems, firewalls, and so on are used, it may be possible to pass or prevent the cyber-risk from occurring.

REFERENCES

Becker, G. S. 1978. *The Economic Approach to Human Behaviour*, The University of Chicago Press.

Böhme, R., and Kataria, G. 2006. "Models and Measures for Correlation in Cyber-Insurance," in *Workshop on the Economics of Information Security (WEIS)*, University of Cambridge, England.

Cohen, L. E., and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* (44:4), p. 588. (https://doi.org/10.2307/2094589).

Courtney, R. H. 1977. "Security Risk Assessment in Electronic Data Processing Systems," in *AFIPS Conference Proceedings - 1977 National Computer Conference, AFIPS 1977*, pp. 97–104. (https://doi.org/10.1145/1499402.1499424).

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).

Kunreuther, H. 1997. "Managing Catastrophic Risks through Insurance and Mitigation," *Philadelphia, Wharton Risk Management and Decision Processes Center*, pp. 1–31.

McCarthy, B. 2002. "New Economics of Sociological Criminology," *Annual Review of Sociology* (28:1), Annual Reviews 4139 El Camino Way, PO Box 10139, Palo Alto, CA 94303-0139, USA, pp. 417–442.

McLennan, M. 2021. "The Global Risks Report 2021," *World Economic Forum*. (https://www.weforum.org/reports/the-global-risks-report-2021).

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).

Pregibon, D., and Hastie, T. J. 2017. "Generalized Linear Models," *Statistical Models in S*, Routledge. (https://www.crcpress.com/Generalized-Linear-Models/McCullagh-Nelder/p/book/9780412317606).