DENIAL OF SERVICE ATTACKS AS DISASTERS

Norman Pendegraft, College of Business and Economics, University of Idaho, Moscow ID 83843
208-885-7157, norman@uidaho.edu
Mark Rounds, College of Business and Economics, University of Idaho, Moscow ID 83843,
208-885-4199, mrounds@uidaho.edu

ABSTRACT

The paper describes a simulation model of denial of service attacks as discrete events of varying duration and intensity which make a system temporarily partially unavailable. This makes them like disasters rather than information thefts. Users are assumed to leave with varying likelihood. The dependence of the likelihood of survival on user loyalty and rate of system decline is illustrated for attacks for varying duration and intensity.

Keywords: Denial of Service, DoS, Simulation, Disaster

INTRODUCTION

Objective

The work reported here is part of program of research examining the behavior of information systems under attack, the attackers and the users of those systems. This paper deals with denial of service attacks (DoS) and treats them, for planning purposes, more like disaster information thefts.

Background

The importance of humans in information security (Infosec) planning was recognized long ago [11]. More recently systems dynamics has been used to study Infosec. See [2] for example. The model used here is based on [10] as extended in [9]. The first considers attacks as continuous processes while the latter considered disasters as discrete events. In the latter paper, disaster arrivals were modeled as a Bernoulli Process (i.e. memoryless on discrete times). Here we consider a DoS attack as only a single event and study the consequences.

DoS attacks are of increasing importance. Verizon [13] reported that DoS attacks "are again at the top of action of varieties associated with security incidents, but it is still very rare for DoS to feature in a confirmed data breach". Nonetheless they are costly. A 2014 study [7] suggested that DoS attacks cost, on average, $40,000 per hour.

Several authors have offered models for evaluating the economics of attacks. A theoretical mathematical model for a DoS included, in addition to the direct costs of the attack and recovery, parameters such as the start and stop times of an attack and loss of customers. [1] They use a deterministic model to calculate total cost for several scenarios.

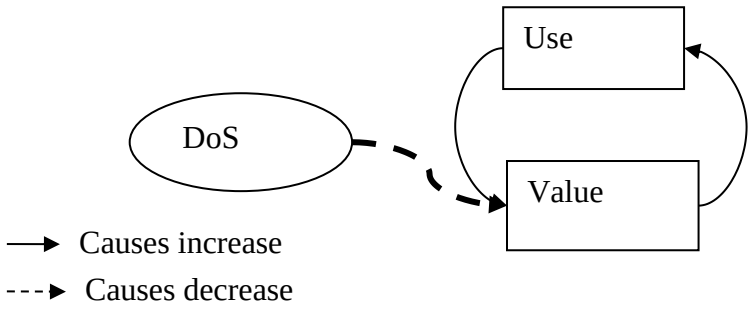
DoS attacks vary both in duration and intensity. Kaspersky [6] reported 2018 attacks lasted from a few hours to several days. Imperva [4] reported that since 2017 attacks have increased in intensity.

We use several of these constructs in the model presented here. The remainder of the paper is organized as follows. The next section describes the methodology. Then we offer the results. The paper closes with a discussion of the results.

METHODOLOGY

The model is illustrated in Figure 1. The simulation was conducted using IThink a tool for continuous event simulation. This extension requires that we include discrete events, and modeling that will take some explanation.

FIGURE 1: BASIC MODEL

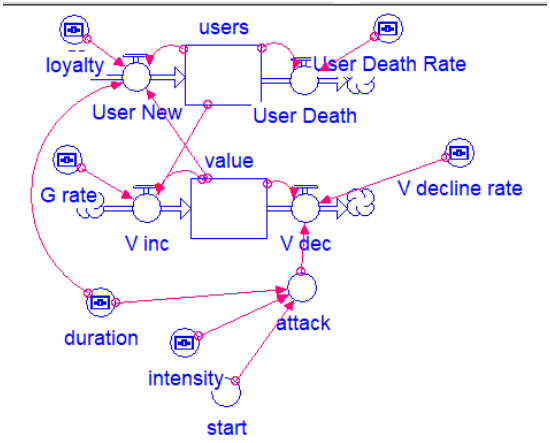


Model Outline

The model assumes that DoS attacks essential render the system unavailable and that users are unable to use the system, or at least are unable to use it the same extent, until the DoS is resolved. Thus a DoS has at least three parameters: at start time, a duration and a severity. We consider each of these in turn. We further assume that users will return to the system based on its value at the end of the DoS and on a parameter (Loyalty) that measures the propensity to return. We assume a homogeneous body of users who have a natural "death rate", and who have a "birth process" proportionate to the value of the system and their loyalty.

In this model we do not consider attackers as separate population nor do we consider security. We also modeled the rate at which system value declines as a parameter.

FIGURE 2: ITHINK MODEL



Parameter Choice and Validation

The parameters chosen resulted in a steady increase in users and value. This was sufficient at present to validate the parameters.

Intensity=1
Duration=3
Growth rate=0.15
UserDeathRate =0.1
Time horizon =30
Intensity and duration were varied

The growth rate of system value was estimated by looking at a number of social media sites that collectively approximately doubled in users in 5 years. [8] This suggests a growth rate of about 15% is a reasonable order of magnitude estimate.

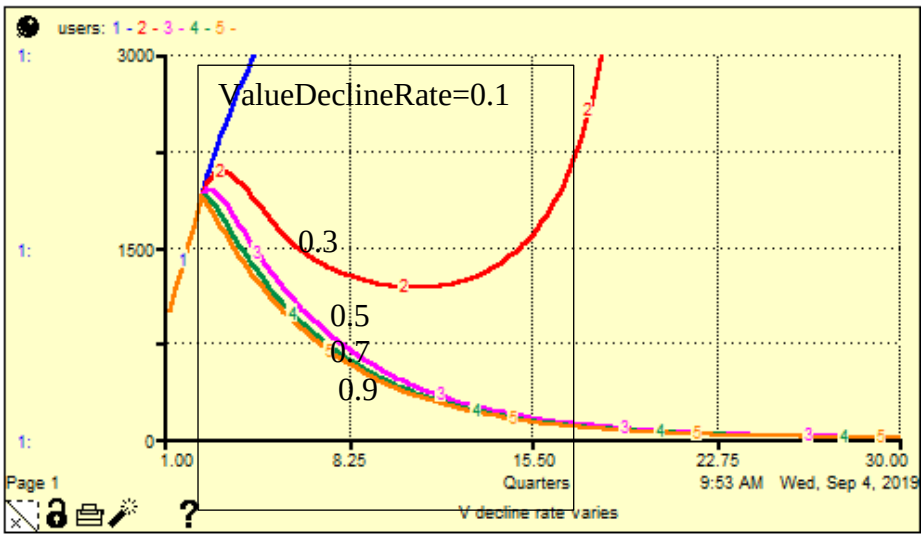
UserDeathRate is an arbitrary choice based on a number of disparate facts. Edison Research [3] recently reported that Facebook has fewer users in the US than they had in 2017. This may be associated with the negative publicity that they have received. Facebook users dropped around 20% from 2017 to 2019. Twitter users dropped more than 20% in that time. While it is almost certain that there is a constant joining and leaving process going on, these are net numbers, i.e. the number who join minus the number who leave. Thus, 10% seems a reasonable order of magnitude estimate.

RESULTS

Figure 3 illustrates a typical result. There are 5 cases in which the V decline rate varies from 0.1 to 0.9 in steps of 0.2. The horizontal access is time and the vertical axis is the number of users. In this case it is noted that for a decline rate of 0.3 or less, that the population will return and the system will survive.

FIGURE 3: TYPICAL SIMULATION RESULT

(INTENSITY = 1; LOYALTY=.9, DURATION=3)

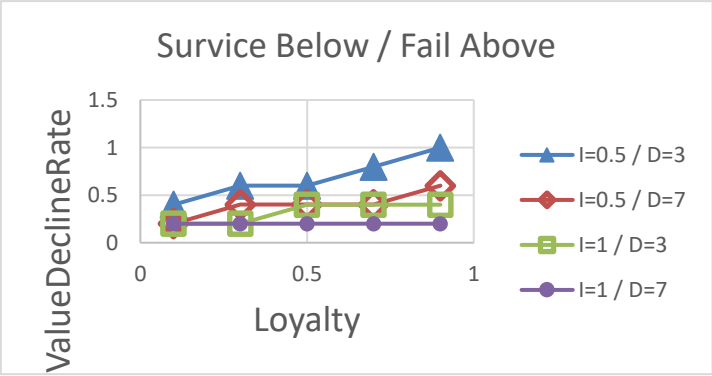


The simulation was run for three major situations.

In the first case (illustrated in Figure 3), Intensity=1, Loyalty=0.9, and Duration=3. In the second case, duration was set to 7, and in the third case, duration was reset to 3 while intensity was set to 0.5.

Simulation results are illustrated in Figure 4. The curves are approximate boundaries separating regions in which the system will survive from those in which it will fail. For example, the middle curve (with squares for markers) represents the case for intensity =1 and duration=3. For systems with (Loyalty, ValueDeclineRate) below that curve, the system will survive. Systems starting with (Loyalty, ValueDeclineRate) above the curve will fail.

FIGURE 4: RESULTS



DISCUSSION

Implications

One of the implications is that the model's value may not be limited to denial of service attacks, but may fit other disruptions. For example, the recent decline in Facebook numbers has been attributed to the Cambridge Analytica case [13]. Evidence suggest that news of a major privacy breach has a similar impact. [5] This also, to us, suggests that treating

Sensitivity

It is clear that the system is sensitive to all of the parameters. This is not surprising. In the specific examples examined here, superficial examination suggests that the system has similar sensitivity to Loyalty and ValueDeclineRate. It is apparent that increasing loyalty improves survival and the reducing VDR or intensity also improve survival. It remains to conduct similar analysis using other parameters.

Limitations

The paper assumes that there is no other response after DoS. In particular, no effort is made by the target system to reach out to users to encourage them to return. Clearly, this is a severe simplification. It also assumes that users are homogeneous.

Future Work

Much remains to be done to make the model useful to managers. Many of the assumptions are strong and need to be relaxed. Remaining assumptions need to be validated against empirical data. The model needs to be linked to other formal security models to bring together a comprehensive simulation of the security space.

BIBLIOGRAPHY

[1] Dubendorfer, T., Wagner, A., & Plattner, B. (2004). An Economic Damage Model for Large Scale internet Attacks. 13th IEEE international Workshops on Enabling Technologies, (pp. 223-228).

[2] Dutta, A. R. (2008). Dynamics of Organizational Information Security. Systems Dynamics Review, 24(3), 349-375.

[3] Edison Research. (2019). The Infinite Dial 2019. Retrieved from Edison Research: https://www.edisonresearch.com/infinite-dial-2019/

[4] Imperva. (2019). Q2 2017 Global DoS Threat Landscape. Retrieved 10 2, 2019, from imperva.com: https://www.imperva.com/resources/resource-library/reports/q2-2017-global-DoS-threat-landscape/

[5] Kenner, S. (2019, Nov 8). Users Stop Engaging With Brands After Data Breaches, Report Finds. Retrieved from eWeek: https://www.eweek.com/security/users-stop-engaging-with-brands-after-data-breaches-report-finds

[6] Kupreev, O., Badovskaya, A., & Gutnikov, A. (2019, Feb 7). DoS Attacks in Q4 2018. Retrieved from kaspersky.com: https://securelist.com/DoS-attacks-in-q4-2018/89565/

[7] Matthews, T. (2014, Nov 12). DoS Impact Survey Reveals the Actual Cost of DoS Attacks. Retrieved from Imperva.com: https://www.imperva.com/blog/DoS-impact-cost-of-DoS-attack/

[8] Ortiz-Ospina, Esteban, (2019). The rise of social media, Our WO=orld of Data, Oxford University, https://ourworldindata.org/rise-of-social-media

[9] Pendegraft, N. (2016). A Simulation Model of INFOSEC Defense Against Natural Disasters. WDSI.

[10] Pendegraft, N., & Rounds, M. (2007). Simulation Model of Information Systems Security. International journal of information security and privacy, 1(4), 62-74.
[11] Saltzer, J., & Schroeder, M. (1975). The Protection of Information in Computer Systems. Proceeding of the IEEE, 63(9), 1278-1308.
[12] Seth, S. (2019, Jun 25). Facebook App Loses a Quarter of Americans. Retrieved from Investopedia: https://www.investopedia.com/news/facebook-app-loses-quarter-americans/
[13] Verizon. (2019). Results and Analysis. Retrieved from 2019 Data Breach Investigation Report: https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/