Economics - Security Metrics

Michiel Doesburg
TU Delft
m.s.doesburg@student.tudelft.nl

Cas Buijs
TU Delft
s.j.m.buijs@student.tudelft.nl

Aleksandra Taneva
TU Delft
a.p.taneva@student.tudelft.nl

Elena Tsvetkova
TU Delft
e.o.tsvetkova@student.tudelft.nl

September 2018

Abstract

For the course Economics of Cybersecurity of the Master program Computer Science at Delft University of Technology, we analyse a certain dataset, name and define the security metrics corresponding to this given dataset. Further, a discussion arises considering the connection between security measures and security metrics. By defining the metrics, as the assignment demands, we investigate and determine the impact and threat of the given data extract. Supposedly, the metrics will give the opportunity to quantify and structure a certain characteristics of the data presented and estimate the value of the components. For the purpose of investigating and reviewing of the metrics, a graphical illustration is presented.

1 Introduction

The concept of exchanging goods and services exists for a long time and with the rise of the internet the offerings have also moved to online platforms, like 'Marktplaats.nl' or 'Ebay.com'. Those platforms are regulated and abide to the laws of the countries they make trade available in but not every platform does that. There exist platforms that allow the exchange of goods and services, which are prohibited by law in the countries they make the trade available in. Online platforms, or also called online marketplaces, that ignore the law are called 'illegal 'underground' marketplaces' as they try to hide themselves in the World Wide Web. Nowadays, there are multiple examples of such marketplaces, like 'Silkroad 3', 'Dream Market' and 'Berlusconi Market'. The existence of these

market raises a security issue from a governmental perspective. The government has the duty to protect the wellfare of society and the safety of its citizens. To make use of more risk management terminology, the safety of its citizens and wellfare of society can be considered the assets that the government values. This also means that the Government is the Defender of those assets in this picture. The existence of illegal, underground, market places harms society in several ways, like the evasion of taxes on legal incomes, which could be used to support the government in fulfilling its duties, or the distribution of forbidden drugs that poses harm to society's health. The government thus has to protect these assets from the criminals that run the illegal, underground, marketplaces, which are the attackers using the aforementioned terminology.

2 What security issue does the data speak to?

The data pertains to 7 (illegal drug) underground market places, with around 3 years of data (2012-2015). The data contains 4 tables which encompass the transaction data of these 7 underground markets:

1. Transaction data between users which includes the hash of the item which was sold, the seller, buyer, marketplace on which the item was sold, date of transaction, order amount, and price paid.

2. Data on the items being sold, which includes a prediction of the category of each item (Benzos, Stimulants, Ecstasy, etc...) per marketplace the total amount sold of each item, from when to where it shipped, and when the item was first and last observed.

3. For each marketplace the total amount of sales, the amount of sales in the last 90, 30 and 7 days, and when the first and last transactions where observed.

4. For each marketplace and user the total amount of sales, the fraction of total sales the user represented, the sales per day, sales in the last 90, 30, and 7 days, the category of the item the user sold most of (Benzos, Stimulants, Ecstasy, etc...), for each category how much the user sold, and when the user was first and last observed.

The security issue is obvious: illegal drugs (and other goods) are being sold via underground markets on the internet. These items have been classified as harmful to society and thus are illegal. These underground markets undermine nations' legal systems around the world, and are harmful to societies. The internet facilitates the illegal trade as it provides easy access to potential customers to numerous illegal substances, while at the same time eliminates the need for an intermediary, thus making it safer for both buyers and sellers to engage in such activities. Furthermore, the great amount of anonymity makes it difficult for law enforcement and international agencies to track and prevent such distribution taking place. The evolving role of underground online markets in

drug retail opens new opportunities for organized crime groups to further their activity in new and innovative ways, earning them huge profits at the expense of society's welfare, but more importantly, of the health of its citizens

3 What would be the ideal metrics for security decision makers?

- Percentage of share the underground market places have in terms of the economical value covered by all market places.
- The growth rates of the illegal, underground, market places.
- Level of harm done to society by the underground market places.
- Level of maturity on protection of the assets against the underground market places.

4 What are the metrics that exist in practice?

Security metrics - existing four types of metrics related to the security, classified from cost to benefit of security:

- metrics, based on controls - measures applied in practice to mitigate risk (physical, organisational, procedural, technical)
- metrics, based on vulnerabilities - how system weaknesses perform during hypothetical attack (threat scenario)
- metrics, based on incidents - the events triggered by an actual attack
- metrics, based on prevented losses - economic impact of the incident, driven by unknown attacker behavior

Further, another classification from cost to benefit of security would be level of the environment threat - from lack of threat to existing such.

5 A definition of the metrics you can design from the dataset

Metrics we can design from the dataset:

- Numbers of buyers in the underground markets
- Number of sellers in the underground markets
- Amount sold per market

- Amount sold per user
- Amount sold per category of item (per market)
- Amount of users per market
- Number of transactions (per market, per user, total)

6 Evaluation of metrics

7 Notes

- Whose security? (Defender) - Government protects the security of society
- Security of which values? (Assets) - Economic impact of underground market - direct (in terms of taxes) and indirect (health problems); Social welfare
- Security against what/who? (Attacker) - Criminals, Illegal good traders

Possible Metrics:

- Growth rate of number of underground markets (own)
- Price rates of the goods
- Change of price per item per year (if possible)
- Revenue per country (choose country, region)
- Amount of sales per market (per year)
- Average income per user per market
- Distribution of categories of item per market (market A sells 80% stimulants, market B sells 30% Benzos, etc...)
- Goods sold per country (amount in USD, fraction of total per category)
- Per country total goods incoming and outgoing
- Revenue made per category of good

Ideal metrics (and why they are ideal - see the impact, take into consideration, resulting in effective measures):

- Total amount of illegal goods sold around the world. (How big is this issue?) - per year/market
- How many users are involved (buying and selling) in these markets (per year, per market, in total)

Ideal metrics allow to illustrate a certain mathematical trend and to measure, estimate, create indications about the risks and threats to the society.

Metrics existing in practice (with reference):
Proportion of items in the marketplace as a function of the number of sellers. What fraction of the total number of items are sold per user (does 1 person sell 80% of all goods, or is there high diversity?). This study observed that no one seller sold more than 1.5% of total goods in Silk road.

8 Conclusion

This section is supposed to be completed for the future official report.
The following conclusion summarizes the main outcomes of the report.

References