Economics - Security Investments

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 discuss security investment strategies for several actors related to the security issue from the previous assignment. We first define our problem owner and present the corresponding risk strategies for it to reduce the security issue. A discussion arises about differences in security performance for the problem owner, which we take are the market owners of underground markets. Then, we look at the other actors that play a role in the security issue, like law-enforcement agencies and the users of the markets and come up with different risk strategies for the actors. In the end we chose the risk mitigation strategy of the problem owner to, using the provided dataset, calculate the Return on Security Investment (RoSI) for.

1 Problem Owner

The security issue measured in our first assignment was the existence of underground marketplaces and the possibilities this offers to cyber criminals to anonymously conduct illegal trade and spread malicious software, thus circumventing the authorities. However, this security issue can also be seen from the other side, which is the issue of law-enforcement agencies going after the people who keep these marketplaces active and trying to put them in jail. Using this second perspective on the security issue, the owners of the different marketplaces are the problem owners. They are responsible for the existence of the

marketplaces and with that carry a big portion of the responsibility to not have the platform's users being caught by law-enforcement agencies.

2 Differences in security performance

Multiple security metrics were developed in the first assignment, but as these did not provide enough depth, a new metric was developed to show the difference in security performance. Our problem owner is, as aforementioned, defined as the owners of the underground markets.

As a market owner there are multiple security factors that you have to take into account, which all influence your security performance. Things that you might come across are the level of anonymity for the sellers, cryptography used to keep the communication secret and the defense of the platform itself. Our metric looks at the security performance as how dependent the platform is on its vendors. If a small percentage of the vendors is responsible for a large percentage of the trade/revenue on the platform, the market is at high risk of losing a significant chunk of its revenue if a seller is caught. Moreover, the most active sellers are more likely to be caught as they produce a larger trail. If each vendor has a relatively low contribution to overall revenue, this risk is smaller, and thus it is easier to maintain the existence of the platform. Our metric evaluates the percentage of vendors of a market place against the percentage of trade it contributes to the total trade of the market per year.

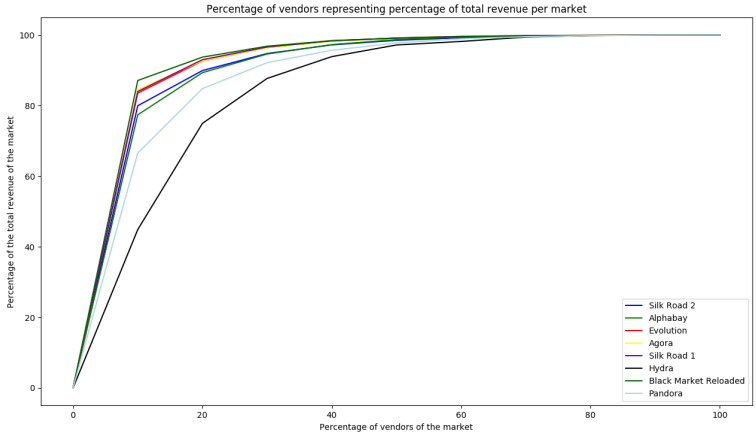

Figure 1: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market.

Figure 1 is an example of the output from our metric. The real outputs for each year can be found in appendix A. As can be seen from the outputs, especially

2014 and 2015, is that most markets roughly follow a 20/80 distribution of their trade with approximately 20 percent of the vendors covering the 80 percent of revenue. The market ‘Hydra‘ has the best distribution between all markets and for that market 10% of the vendors cover almost 50% of the trade on the market. The worst market is ‘Alphabay‘ where 10% of the vendors cover 90% of the trade on the market, which makes this market very vulnerable to attacks on its vendors from law-enforcement agencies. The same coverage would require around 40% of the vendors from the ‘Hydra‘ market. It shows that those markets with the worst distribution of their trade over their vendors should come up with ways to mitigate the risk of losing their biggest sellers by an attack from law-enforcement agencies.

Aside from percentage coverage of vendors, it is important to take into account the absolute number of vendors for markets as well. If 10% equals 100.000 vendors then this is safer compared to 40% which equals 10 vendors. Figure 2 shows the absolute number of vendors and it becomes clear that the market ‘Hydra‘ has such a small number of vendors that the top 10% of vendors refers to 3 vendors on this market which cover around 50% of the trade. Compared to the market ‘Alphabay‘ where more than 300 people cover 90% of the trade. Using both graphs it becomes clear that the security performance of ‘Alphabay‘ is better than that of other markets as their distribution looks similar but ‘Alphabay‘ has a considerable larger number of vendors than the other markets. This means that a larger number of vendors cover the same percentage of trade when comparing ’Alphabay’ to ’Hydra’.

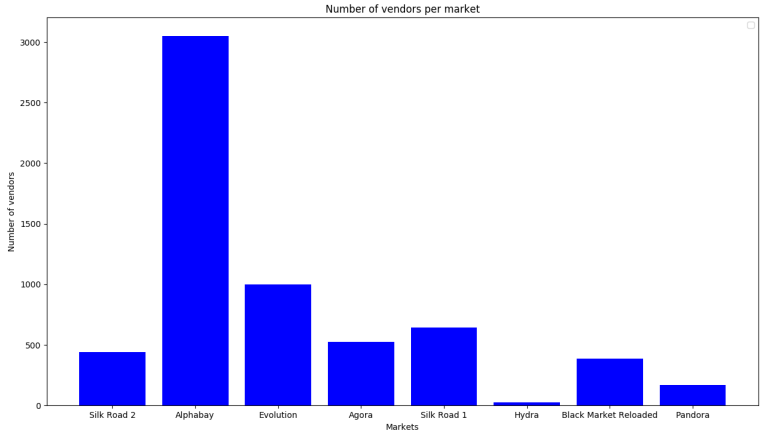

Figure 2: Number of vendors per market

3 Reducing the security issue

An important task for the problem owner is selecting an appropriate risk management strategy to adequately deal with the security issue at hand. Decision makers managing cyber risks can make use of four strategies deployed in general risk management [1]:

- Risk mitigation: involves taking preventive measures by implementing risk controls and containment measures, either on technical or on organizational level, and periodically modifying them in order to meet new security requirements. Nevertheless, reducing completely the risk of a security breach is not practically feasible or financially justifiable considering the decreasing marginal returns of security investment [2]. Therefore, usually there is some residual risk present.

- Risk acceptance: this strategy is deployed in advance, when considering that the losses from taking a specified risk would be acceptable and these actions are not against the law of the particular country, and are in line with the other activities of the organization.

- Risk avoidance: consists in not participating in certain activities in order to avoid taking the risks associated with them altogether, trading off any potential profits from these activities.

- Risk transfer: most often cyber insurance; comprises transferring the risks to an external party which is to compensate financially the organization in case losses are realized in the future.

Taking into consideration the previously specified problem owner: the owners of the underground markets, the most suitable strategy open to them would be that of risk mitigation. Market owners can try to contain the damage a potential law-enforcement operation could have on the functioning of the marketplace by implementing various measures. Most of these are aimed at protecting the anonymity of the users, and therefore their traceability, such as hosting the platform on an anonymous Tor server, or making use of private chat rooms [5]. Members of such marketplaces are required to use proxies or virtual private networks (VPNs), in order to protect their identity and that of the other users. Such actions could limit the damage a market infiltration or exposure of data could cause. Another measure to increase the accountability of the market's users is by employing reputation and referral systems or having strict entry requirements, so as to ensure the members on the platform uphold the principles of the cyber criminal community. Monitoring the behavior of new or suspicious users is another potential option for the market owners, as well as removing user accounts, which have not been accessed for more than a certain pre-defined period of time. Market owners should also take measures to encrypt sensitive details about both sellers and buyers, invest in secure hardware and software, and regularly monitor for any signs of data loss.

Accepting the risks related to possible actions of law-enforcement agencies is another potential strategy, albeit not as suitable. Depending on the size and number of vendors active on each marketplace, risk acceptance could be a viable option, especially for owners of markets where the trade is more evenly spread across a higher number of sellers, such as "Alphabay", and losing some vendors would not present such a threat to the overall business on that market. Nevertheless, there could be other indirect negative effects: loss of data, loss of reputation, which could affect the market in unexpected ways, which is why this strategy would be inferior to the first one.

Market owners could try to avoid the risks associated with running illegal activities by shutting down the underground markets altogether. However, this would be in contradiction with the sole purpose of the existence of these marketplaces: to provide a platform for those willing to participate in the free exchange of illicit goods and services. By not taking this opportunity, they would also forgo any potential profits from offering this service. Hence, risk avoidance is a strategy theoretically possible, but not applicable in practice.

Risk transfer would not be a strategy which the marketplace owners could follow, as there is basically no external partner who could take over the potential risks, as well as provide financial compensation for any losses incurred on their behalf.

4 Actors to influence the security issue

There are multiple actors that are capable of directly or indirectly influencing our security issue. The problem owners have as a main responsibility to keep the illegal trade undisrupted by securing their markets and preserving the anonymity of their users. Besides the problem owner there are several other actors that have some degree of influence regarding the security issue and they will be explained separately.

The first actor, besides the problem owner, are the law-enforcement agencies. They are the threat that the market owners defend themselves and their users against. The law-enforcement agencies can investigate markets, arrest users or intercept goods (if not digital in nature). Through these actions they can (in)directly influence the existence and operations of the market.

Another actor, in the government area, are the law makers. The problem deals with the security issue that something occurs which is prohibited by law, the law makers are responsible for defining the law and thus have a great influence on the matter. By changing the law they could remove the security issue altogether or they could influence the capabilities of the law-enforcement agencies. By using the law they can also have a direct or indirect influence on the buyers and sellers, who could abandon the market places as a result of new laws being

created or old laws being removed.

Finally, the users of the markets (buyers and sellers) have a degree of influence on the problem. The existence of the marketplaces gives rise to the security issue but if there was nobody making use of the market there would not be much to protect. Moreover, the user's security behaviour (use of privacy enhancing technology) affects their chances of being caught, and thus affects the market.

5 Risk strategies

In order to evaluate the risk strategies in security we rely on the four possible instruments in risk management, which have been explained in section 3. Each strategy is used for each actor if applicable, leading to an overview of the various strategies that actors could make use of. As those concerning the problem owner have already been discussed, this section focuses on the strategies for the other actors.

5.1 Law-enforcement agencies

The first actor recognized in the previous section as having an influence on the security issue are the law-enforcement agencies. They have the responsibility of upholding the law and making sure all members of society adhere to it. As this is their main responsibility and the existence of underground markets is an outright violation of the law, it is not an option for them to follow a risk acceptance strategy. Avoiding the security issue is not possible either as it would mean they have abandoned their own duties, something a governmental agency is not allowed to do. In addition, it could also be considered unethical for them to do such a thing. As we are dealing with a governmental agency, a risk transfer is unlikely as a possibility as no insurance company would insure a nation against losses on its economy. This would make the insurance company bankrupt in an instant.

The only option available for the law-enforcement agencies is that of risk mitigation. Considering the markets, there exists a small group of vendors who cover the majority of the trade (in terms of revenue). The law-enforcement agencies could focus on identifying these particular vendors as a preventative measure or they could target the hosting organization of the platform so as to take it offline, in order to limit access to the market.

5.2 Law makers

Another actor identified in the previous section are the law makers. By creating laws they have the option of making the security issue disappear overall. As

the law makers have more freedom compared to the law-enforcement agencies, they could make use of more risk strategies. Although, risk transfer would not work in their case as they have the responsibility of designing a proper legal framework. Risk avoidance is also not an option as it would result in no law to be made as every law could be violated at some point.

Risk strategies which can be used are risk mitigation and risk acceptance. When designing the law, it is already taken into account that someone might violate it. Law makers could opt for a path in which certain minor violations of the law would not be punished, relying on the good nature of the country's citizens. Law makers could also try to mitigate the problem, by designing punishments for violating the law to scare users away from the market. Moreover, they could devise a law that forces involved parties, like hosting organizations, to comply with take-down requests of law-enforcement agencies when needed.

5.3 Buyers on the market

Another actor are the users of the markets. If a market becomes 'dangerous' for buyers and they leave, it would halt the flow of trade and hence, threaten the existence of the market itself. In addition to illegal, legal goods are also traded on the markets, which means that paying taxes can be avoided. Buyers would like to stay anonymous and thus risk acceptance is not appropriate. Risk transfer is not possible either as there is no existing insurance policy for violating the law.

Risk avoidance would be possible, meaning that the buyers would stop their activity on the platform. Another strategy would be that of risk mitigation by protecting their identify and limiting their vulnerability. By participating in discussions and analyzing the feedback provided by other buyers for sellers, they could identify the reliable sellers.

5.4 Sellers on the market

Next to the buyers, there are the sellers. By choosing a market to conduct their business on, they could make it thrive or by avoiding it: make it disappear. Sellers, just like the buyers, do not have the option of accepting or transferring the risk. For the same reasoning as above but from the view of the sellers.

Risk avoidance could be possible by stopping selling goods altogether, though this could possibly harm the personal lives of the sellers. A risk mitigation strategy of keeping their identity and location as secret as possible would be more suitable. They could choose platforms with a better reputation and higher security level, like invite-only markets, to prevent a potential arrest.

5.5 Different strategies

Not every party can make use of the same risk strategies, which has to do with their responsibilities and duties but also with their ethical position towards the issue. Different actors may hold different, possibly opposing, values, which could motivate them to act in conflicting ways. The nature of the actor also plays a role: risk transfer is possible for small organizations but almost unthinkable for whole nations, as the potential losses cannot be covered by any individual insurance company. All these factors have to be taken into account, which leads to different strategies to be applied for different actors, with some applicable to multiple actors.

5.6 Changes in risk strategies

Risk was introduced initially with the creation of the first black market (officially during The Second World War). As technology developed, so did the markets, and that led to the creation of the first online market - Silk Road in 2011. The technology and the instruments to mitigate this risk evolved, however that same technology and those instruments are also available for the creators and administrators of the underground markets. Risk mitigation in this structure leads to a vicious circle which should be broken by changing security strategies in such a significant way, that the black market cannot cope with. Probably, in the future, with the emerging use of the blockchain technology and quantum computers a change could be seen.

6 Return on Security Investment

After identifying possible strategies for the various actors, a closer look is taken at the strategies that the problem owner has to reduce the security issue. In section 1 multiple strategies were mentioned but here the focus lies on the risk mitigation strategy the problem owner could apply. To reduce the risk of the vendors, of which a small part covers the majority of the trade (in terms of revenue), the market owners can offer a VPN service to their users. This would aid them in anonymously making use of the market and reducing the risk of their identification by, for example law-enforcement agencies. This strategy is further used to calculate the Return On Security Investment (ROSI).

First it is important to get an overview of what this measure costs. There are both direct costs, for acquisition, deployment and maintenance of the control, and indirect costs, like lost time for having to connect to the VPN. The indirect costs are so few and insignificant in terms of money compared to the direct costs that they are not considered further. For the direct costs of the measure to use a VPN, already operating services could be utilized. Meaning that the market owner does not have to bear the costs of deployment and maintenance and only pays for acquiring the VPN. A VPN would cost $100 per year per user, although it can be bought in bulk to reduce the price to $30 per year per user[4]. To use

the ‘Alphabay‘ market further for the calculation, with around 3000 users this would make the total cost of this measure $90.000 per year.

What is needed next is to know what benefits this control will yield to the market owner. This benefit consists of prevented losses from incidents, where an incident would be an arrested vendor of the market in this situation. Using the provided dataset, we calculated the mean revenue for each seller to be $5270 with a standard deviation of $38.730. Using an 80% confidence interval shows that the average seller on these underground markets sells goods for a total revenue of $4600 - $6000 per year. As market owners earn money by charging a small fee, which is unknown for us, we assume the transaction fee to be 15% of the transaction value, which is $690 - $900 per vendor per year. For ‘Alphabay‘ with around 3000 vendors this means $2.070.000 - $2.700.000 revenue per year for the market owner. A single arrested vendor only accounts for $690 - $900 in losses but this takes the uncertainty into account. The real revenue made for a specific vendor can differ as the standard deviation is large but we assume it to be as aforementioned.

It is also important to note something about the probability of a vendor being arrested, which mostly depends on the behaviour of the attacker. In this case: the law-enforcement agencies, and we could find no information related to this probability. To simplify this, it is possible to model the attacker as a random variable and create a probability loss function to clarify the probability of an incident. However, our dataset does not give any insights into occurred incidents and thus we have not the data necessary for creating such a plot. To still continue with the ROSI calculation, we assume the chance of a random user to be caught is 5% in a year without the control in place. With the VPN in place, this chance goes down to 0.5% in a year. This means that for ‘Alphabay‘ around 150 users are caught in the situation of no VPN and only 15 users are caught after the control has been put in place. In the case of no VPN it would result in a loss of $103.500 - $135.000 and after the control has been put in place the losses would only be between $10.350 and $13.500. Thus the benefit caused by this control can be calculated as been between: $103.500 - $10.350 = $93.150 and $135.000 - $13.500 = $121.500 using the 80% confidence interval of which we take the average for further calculations. The average is: $107.325.

We use the following formula to estimate Return On Security Investment, as defined by [3]:

$$\text{ROSI} = \frac{(RiskExposure * \%RiskMitigated) - Solutioncost}{Solutioncost}$$

$$\text{Lower bound: } \frac{\$93.150 - \$90.000}{\$90.000} = 0.035,\ 3.5\%.$$

$$\text{Upper bound: } \frac{\$121.500 - \$90.000}{\$90.000} = 0.35,\ 35\%.$$

The risk strategy would thus lead to a positive Return On Security Investment between 3.5% and 35%.

7 Conclusion

For the purpose of this report, we have defined the problem owner as the market owners for our security issue: defending online underground markets from law-enforcement agencies, we have considered the different actors that influence the issue and their corresponding strategies. Therefore, we address the problem of existence of the underground markets from the perspective of the market owner and we refer to the strategies they can follow to reduce the risk. Next, by mapping the risk strategies to the other actors (law-enforcement agency, law maker, buyers and sellers), we describe the approach they can adopt individually to tackle the problem.

Then, by the calculating from the market owners' point of view of the ROSI (Return on Security Investment) for our chosen risk mitigation strategy and making estimations of the cost and benefits, we can analyse whether applying the chosen strategy will be effective. A benefit for the market owner from applying the chosen strategy will be that the possible profit could rise up to 35%. A potential negative apsect to name is that the possible return on the investment is only 3.5%.

Finally, a lot of factors can influence the performance of the system to protect the users. In this case, the estimated benefits of providing VPN for the users can be argued with. Undoubtedly, the security of the users will be increased but it is for the market owner to forecast the consequences of not taking action or not and hence the risk mitigation of reducing 10 times the possibility of seller to be arrested is significant and has to be taken into consideration.

References

[1] R. Böhme. Security metrics and security investment models. In *Advances in Information and Computer Security*, pages 10–24, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[2] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[3] W. Sonnenreich, J. Albanese, B. Stout, et al. Return on security investment (rosi)-a practical quantitative model. *Journal of Research and practice in Information Technology*, 38(1):45, 2006.

[4] H. Staff. How much does a vpn cost? `https://www.howmuchisit.org/how-much-does-a-vpn-cost/`. Last updated: August 14, 2018.

[5] C. Wueest. Underground black market: Thriving trade in stolen data, malware, and attack services. `https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services`. Accessed: 2018-10-06.

Appendix A

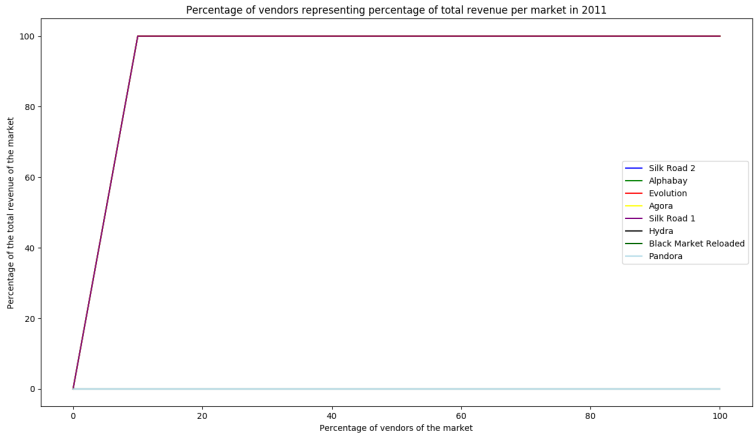

Figure 3: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2011.

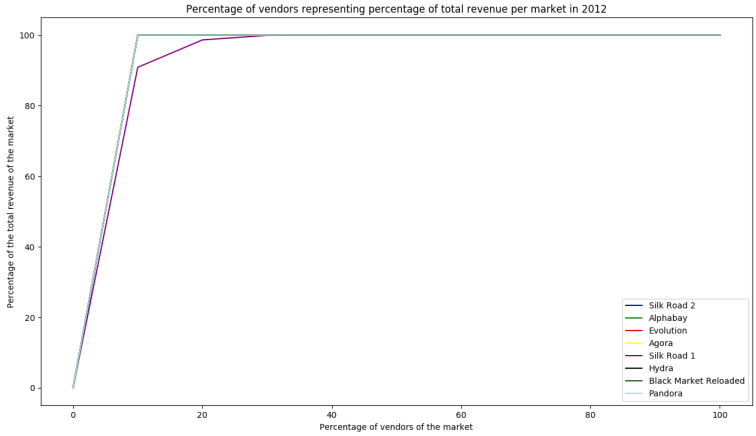

Figure 4: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2012.

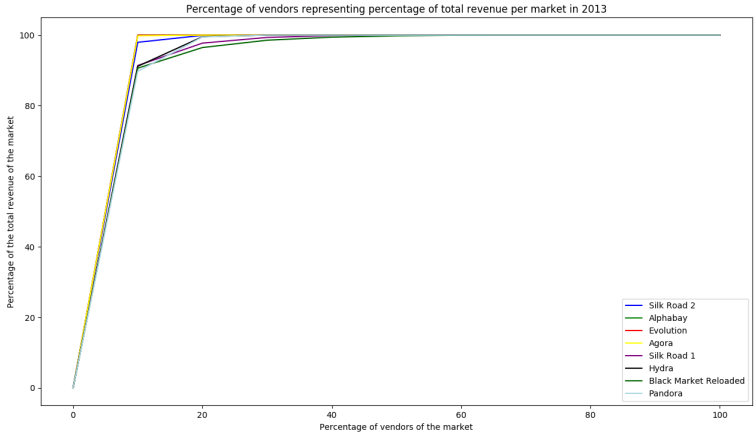

Figure 5: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2013.

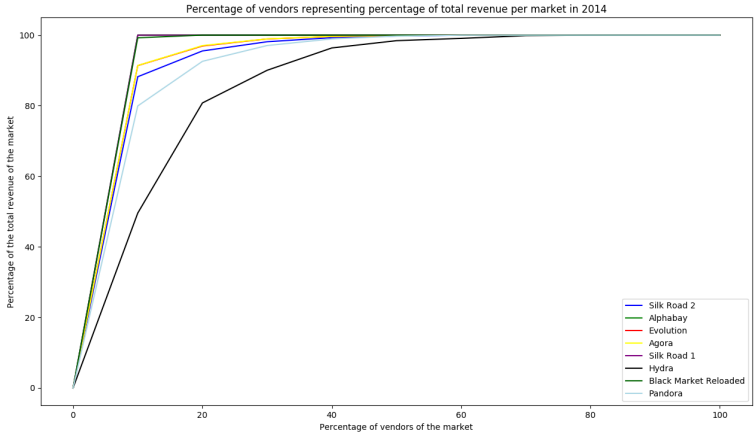

Figure 6: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2014.

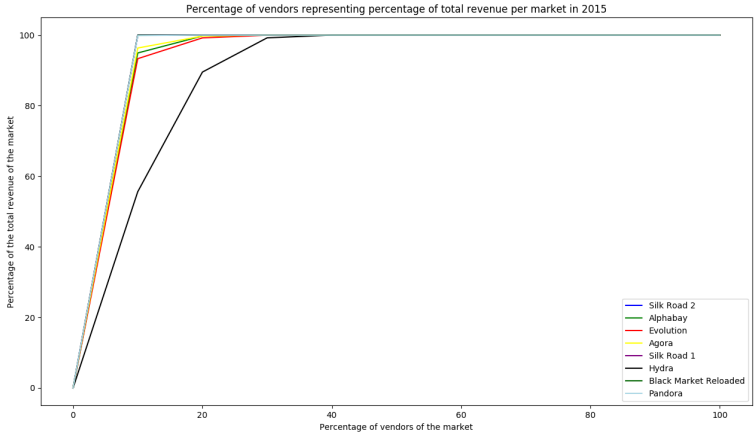

Figure 7: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2015.

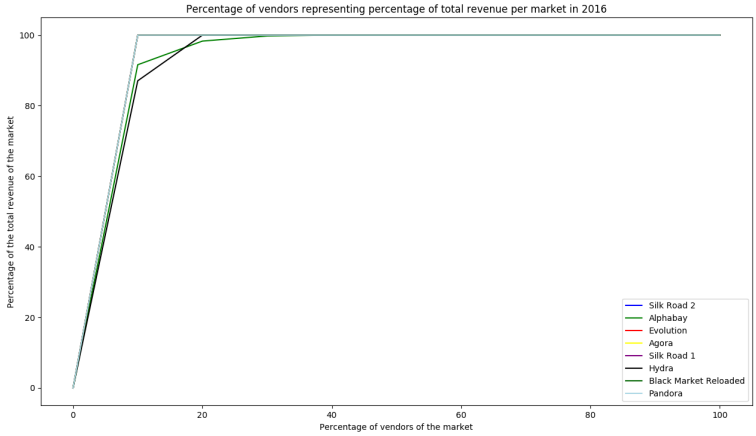

Figure 8: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2016.

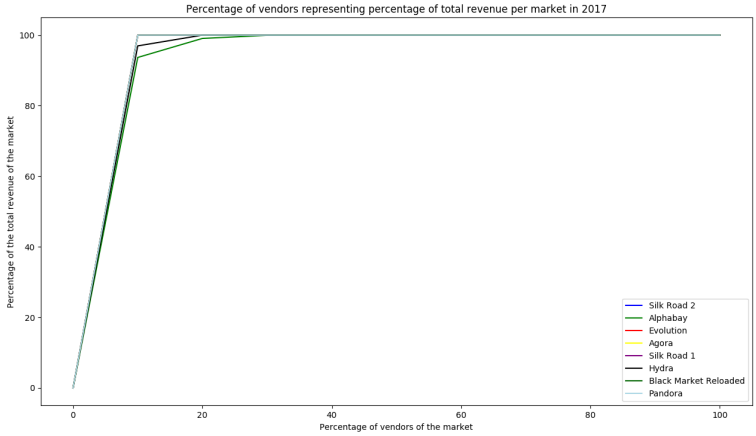

Figure 9: Percentage of vendors on a market place against the percentage of trade the vendors contribute to the total trade of the market in 2017.