Economics of security

Assignment block 3 – Group 2

Akbar Aryanto (s1770705), Amit Gupta (s1637614), Manish Kumar (s1858882),
Vasileios Merdis (s1789309), Jonathan Quigley (s1844261)

Final Paper
Date: Oct 17, 2016

1. Problem Owner

In the previous assignment, we described how ASNs are the prime owners of the problem as they are in an empowered state of taking decisions which can lead to mitigation actions. However, zooming into the situation explains that not only ASNs but the network providers at every node are equally important problem owners.

We looked for metrics which could describe the security issue of IP spoofing, and provide the ASNs some insights to remediate to it. The metrics we produced were based on the tests of the Spoofer project, which allows any and end-user to test his operator's network.

Our metrics measured the percentage of positive and negative tests for all Autonomous Systems of Netherlands available in the dataset. Here, we suggest to use a metric based on **the number of spoofable addresses originating from an AS compared to its size.**

In this assignment, we will focus on the actors impacted by this security issue, and especially on the problem owner. **We identified the problem owner as the network operators**, because they have the ability to implement Source Address Validation (SAV) solutions to prevent IP spoofing. However, they are not the main impacted actors of the issue, which are more likely victims of DDoS attacks using spoofing.

2. Differences in security performances

An interesting metric would be the evolution over the years of the number of AS which allowed spoofing and those who implemented SAV.

Unfortunately, we only have data from the past few months, which is not sufficient to draw a trend in security performances. Nonetheless, we produced a metric which is the number of spoofable IP addresses originating from an AS, function of its size (in terms of number of IP addresses).

Because the information is not directly present in the dataset, we had to manually collect the size of each AS, and therefore we only focused on ASs from the Netherlands. This means the data is maybe not fully representative of the situation in other countries.

Here are two graphs, the first one projecting the number of spoofable addresses originating from an AS compared to its size, and the second one showing the number of spoofable and non spoofable ASs sorted by ranges of size .

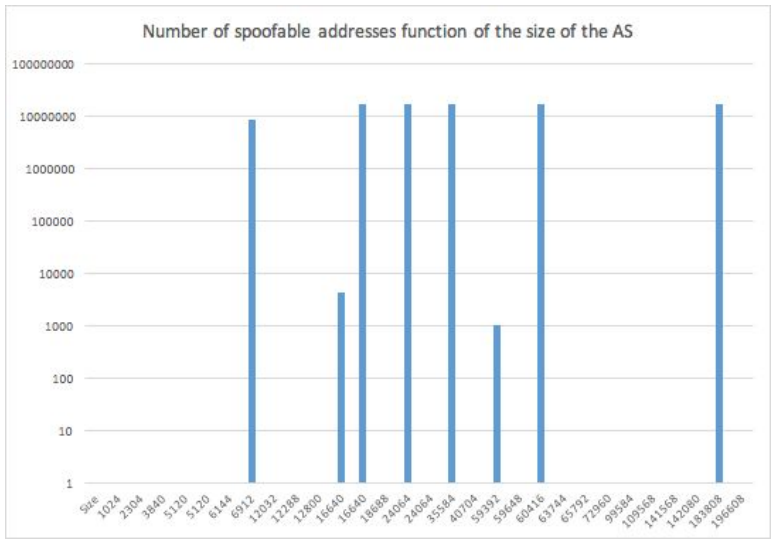

fig: Number of spoofable addresses (function of the size of AS)

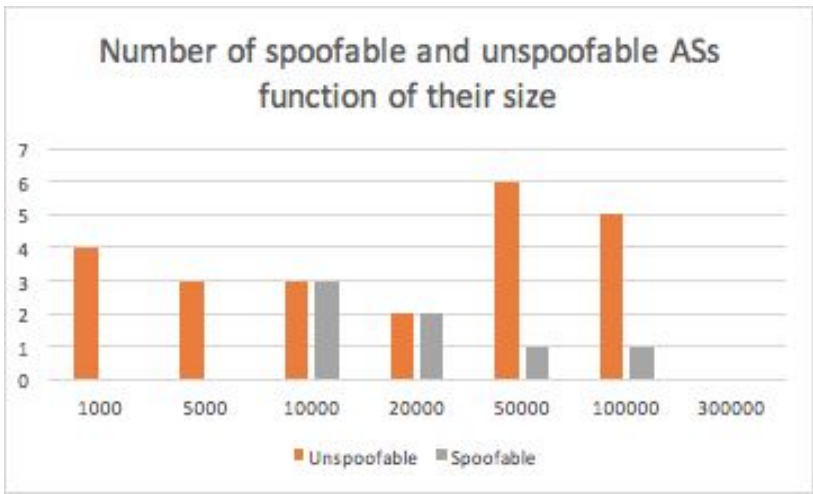

Fig: Number of spoofable and unspoofable ASs (function of their size)

The first assumption we could make from this metric is that larger ASes are more likely to implement Source Address Validation, as they have more resources than smaller ones.

However, we would have to confirm this trend with larger data to make some reliable observations. For networks operators, this metric could tell them how they behave compared to their pairs, and produce some kind of shame effect if they do not conform to the others' standarts. Moreover, it would be relevant to produce another metric based on the transit degree of ASs, as it indicates if the AS is more at the edge of the network or in the core of it. As SAV should be implemented at the edge, where the end users are connected, the metric could show if some ASs which are spoofable, however it is normal for them as they are Transit ASs.

Another interesting Metric that we could figure from the data is that all AS which are spoofable (specially the netblock from neighbouring AS) are also spoofable within the source AS.

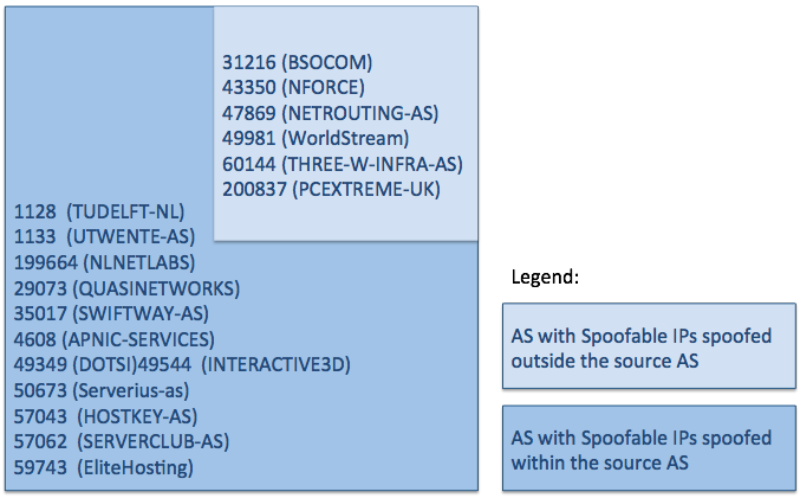

fig: ASes with spoofable IPs inside and outside the source

3. What risk strategies can the problem owner follow to reduce the security issue?

Information security risk management can be described as the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment. As a result, the identification, mitigation, and management of **risks to information security** are vital for the future sustainability of any organization. The ISO 27001 sets guidelines and assessment standards for the possible strategies for risk management.[1]

In general, the possible risk management strategies can be categorized under following four potential decisions as under:

1. Risk Reduction/Mitigation: to try to reduce the risk or the probability of its occurrence to the least possible;
2. Risk Acceptance: strategic decisions to not trying to fix the risks and live with them for the time;
3. Risk Avoidance: to avoid the situations/features that lead to the risk;
4. Risk Transfer: utilizing insurance/assurance agencies to take care of the risks and its possible damages; e.g. insurance of assets;

As mentioned earlier, the problem exists in every node of the network. Spoofer [2] suggests that each node (router/firewall/switch) with mitigational filters can reduce the risks.

In the given context, considering the problem owners to be the network providers, we can describe the possible risk strategies under following situational decisions:

1. **Risk Reduction-** The network providers can take up many steps to reduce the risk for their customers for being spoofed. Some of the adopted techniques are mentioned below, however, the bottomline of the decisions are defined on the basis of the investment to profit ratios.
    a. Ingress Filtering

i. It deploys filters at the edge of the network to discard packets whose source IP is not in the edge network. Unfortunately, its effectiveness depends on the universal deployment. In reality, the deployment is slow due to administrative burden, lack of incentive and so on. Ingress firewalls for preventing the wider Internet from accessing services in possibly malicious ways.

b. Egress firewall
   i. There is another type of firewall called an egress[1] firewall, or a firewall that filters outbound connections from a machine to the internet.

c. Source Address Validation (SAV)
   i. The network provides can deploy SAV to ensure that every packet received and forwarded hold an authenticated source IP address.

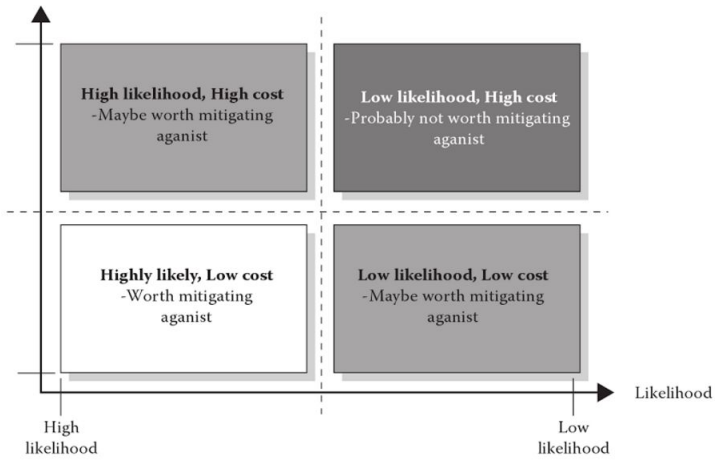

Figure: Risk Analysis [3]

2. **Risk Acceptance -** Most likely alternative to transferring the risk is to retain a risk - relying on our internal resources to cover negative returns. Risk acceptance is a form of toleration of the risk. Practically, it is not possible to 100 percent of the risks for 100 percent of the times. Upto a certain degree of possibility, the risks are reduced, but then in many cases a part of the risk is accepted as well. For example, in situations when the cost of investing in the resolution of the risk is much more than the value of the asset that needs to be protected, then the owners believe in loosen their investments to a certain degree of attacks. Instead, they try to focus on the prime threats which seem to have even bigger impact.

   The decision makers also use multiple tools to understand the threat scenarios and make risk management decisions for their assets .In figure below, we give a snapshot of one of the risk management flowchart that is offered by CORAS tool. [4]

[1] https://en.wikipedia.org/wiki/Egress_filtering

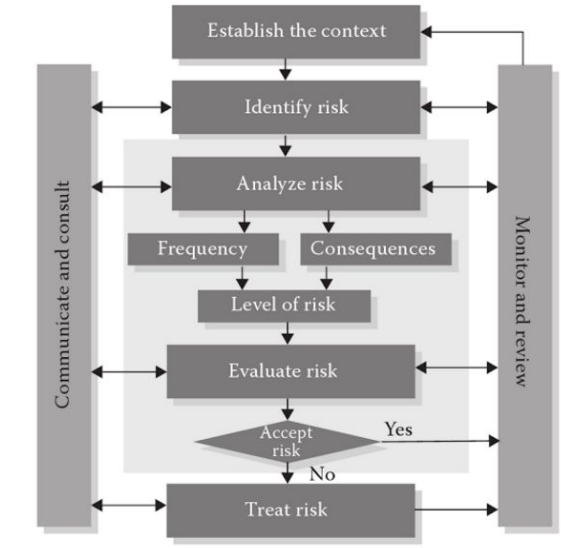

Fig: CORAS risk management workflow [4]

3. **Risk Avoidance -** At first sight, Risk Avoidance seems to be the most simple of all the possible risk strategies. However, as we move closer, it is evident that avoidance can also lead to a great loss to the prey's business. For example, if a network provider limits the bandwidth and blocks some traffic to the end user due to decrease the risk of attacker from outside networks will decrease the speed and performance of the internet and somehow can disturb the legitimate users using those networks services.
4. **Risk Transfer -** Transferring the risk means that we transfer some of the risk to another actor. We could pay an insurer for a commitment to cover our losses, rely on some guarantor to compensate us for the possible happenings, share the risk with business partners, or share risks with contractors. [5]

   It is understood that the more risks are covered by the owner, the better it is. However, the network providers also tend to buy insurance for assuring the delegation of the outcomes of the possible risks. There are multiple ways in which a Network Provider can transfer the responsibilities of the risk to outsourced third parties, clients, service providers or insurance companies. For sure each choice of notion costs in its own way.

4. What other actors can influence the security issue?

There are other actors that can be influenced by the security issue we are focusing (spoofing-based denial of service (DoS) attacks). Such as

1. **The Country,** because their reputation is on stake.
2. **The Victim,** who basically pays all the losses and bear the cost of a DDoS attack and their Preventions in some cases.

The Domain Name System (DNS) is a another such actor and a critical element of the Internet infrastructure can be influenced by the security issue we are focusing (spoofing-based denial of service (DoS) attacks).

Even a small part of the DNS infrastructure being unavailable for a very short period of time could potentially upset the entire Internet and is thus totally unacceptable.

Unfortunately, because DNS queries and responses are mostly UDP-based, it is vulnerable to spoofing-based denial of service (DoS) attacks, which are difficult to defeat without incurring significant collateral damage. The key to prevent this type of DoS attacks is spoof detection, which enables selective discarding of spoofed DNS requests without jeopardizing the quality of service to legitimate requests.

5. Risk strategies that the actors can adopt to tackle the problem

As we mentioned in the previous section, there are some other actors, except the problem owner, that can influence the security issue by adopting different strategies. These strategies differ from the strategies that the problem owner adopts and sometimes they may clash with them.

The country's reputation is a very sensitive issue. The government of each country should take some measures in order to avoid and mitigate in the first place the risk caused by spoofing based on denial of service (DoS) attacks. The authorities of each country should firewall the whole country to disable attackers of other countries to have access on it. Another measure for avoiding the risk should be to filtering and blocking malware spreading by e-mails among the country. The countries should invest some money in order to train the companies and also the users of Internet about the topic of IP address spoofing and how to protect from being attacked. This would help to reduce the impact of a risk and as a result to guarantee the country's reputation in high levels. Furthermore, a country can protect each companies and then each citizens by applying some laws against IP spoofing, so the attacker would think twice of breaking them. Finally, in order not to downgrade the reputation of a country, the government and the security department of a country should not accept or transfer the security issue. They should not allow their ASNs to be spoofable as the reputation of a company or of the major companies and brands from a country ends up having a decisive influence on the reputation of that country in general.

Another actor that can be influenced by the security issue is the victim. And a victim can be considered both the target IP and also the IP that the attacker uses in order to hide his own. Strategies used by victims are limited in the category of risk mitigation and transfer. One of the easiest methods for the victims to mitigate IP Spoofing, is by installing a firewall or a filtering rule, which filters out all packets coming from the outside of a network, but having an IP Address belonging to a system within the internal network structure. Although there are some methods that the victims can adopt while trying to mitigate the risk of IP spoofing, not all of them are following the easy way. They prefer to transfer the risk toward the ISP.

The following are the strategies being used in practice by DNS server. In all these strategies, a DNS server sends a distinct cookie to each requesting host, and the requester associates each request it sends to the DNS server with the server’s corresponding cookie. By checking the cookie that comes with each incoming request, it is possible to determine if a DNS request indeed originates from source address indicated in the packet. However, how to introduce these cookies in a way that is transparent to the existing Internet infrastructure and incurs minimal performance overhead is the design challenge.

1. **DNSSEC**

   The DNS Security Extensions, it's much easier. DNSSEC stores cryptographic keys and digital signatures in records in the namespace. These are positively enormous.

2. **Hop count based mechanism called HCF to detect spoofed packets.**

Servers can learn the normal distance (hop count) of their clients. It is assumed that there is no easy way for an attacker to learn the distance between a server and its clients, thus the server can detect spoofed packets because of the incorrect hop count in the packet.

3. TTL to detect spoofing.

Overall this is a good solution. But some drawbacks may hinder its application to DNS because of the false negative ratio and hop count learning issue.

4. Ingress Filtering

It deploys filters at the edge of the network to discard packets whose source IP is not in the edge network. Unfortunately, its effectiveness depends on the universal deployment.

Have the strategies changed significantly over time?

In an age of Botnets where an attacker has a layer of abstraction behind a command and control server, some people think that IP Address Spoofing is no longer an issue. When in fact the reality is the opposite, IP Address Spoofing remains a real problem to defend against. In some cases, IP Address Spoofing is necessary for an attack's success, where it provides an additional layer of anonymity and protection for a botnet, e.g. DNS DDoS attack.

Internet Service Providers (ISP) have changed significantly over the last decades in order to reduce the risks concerning the security issue. Consumers are pressing the organizations and the companies to take measures against IP address spoofing, because they are the real victims of a possible attack. Thus, ISP changed their strategies over time as they want to ensure more security to their clients and also to improve their reputation. As we mentioned before, a country's reputation affects and is affected by the reputation of its companies. This leaded the countries to make some changes in risk strategies in the past years. There has been an increase regarding the issue of security and more money have been invested to deal with this matter.

6. Calculating the Return on Security Investment (ROSI)

It is clear that DDoS has been an uncontrolled threat to our present generation network system. Moreover, regardless of the type of DDoS attack, current techniques used to deal with them fall short in terms of mitigation and ensuring business continuity. Some of the more popular DDoS responses-such as "blackholing" and routing filtering-are not optimized to deal with the increasingly sophisticated attacks being seen today. IDSs offer some excellent attack-detection capabilities, but cannot mitigate the impact of the attacks. Firewalls offer a rudimentary level of protection but, like blackholing and routing filtering, they were not designed to protect against the types of advanced attacks that are so common today. Still other strategies, such as over provisioning, do not provide adequate protection against ever larger attacks, and they are far too costly as a DDoS prevention strategy. [6]

a. Let us consider that we are a **medium scale network provider enterprise** and we understand the risk of spoofing DDos from our network. Being a medium scale company, with more than **200k customers**, we have enough budgets to plan our risks than losing bandwidth, trust and QoS for our services.
b. Since, we don't want DDoS spoofed IP packets to originate from our systems and subdomains, we would like to follow the **Risk Reduction Strategy** pertaining to the foreseen problems.
c. We tried to enlist the popular solution systems available in the market who offer to control and reduce the problem of IP spoofing and at the same time offer reliable and efficient routing. To the top of our list is an anti-distributed DoS gear are **Cisco Solution set.** [7]
d. The Cisco solution set includes two distinct components-the **Cisco Traffic Anomaly Detector (TAD) XT** and the **Cisco Guard XT**, working together, deliver complete DDoS protection for virtually any environment.
e. The Cisco Guard XT 5650 offers:
    i. Detecting the DDoS attack
    ii. Diverting the data traffic destined for the target device to a Cisco appliance for treatment
    iii. Analyzing and filtering the bad traffic flows from the good traffic flows packets, preventing malicious traffic from impacting performance while allowing legitimate transactions to complete
    iv. Forwarding the good traffic to maintain business continuity
f. The high-performance *Cisco Traffic Anomaly Detector XT* monitors attack flows at full gigabit line rates-enough to identify more than 100,000 sources per device in a single attack, providing robust protection for large, high-volume environments against distributed attacks.[8]

g. The Cisco Guard XT systems offers protection against [9]
    1. Spoofed and non-spoofed attacks
        a. TCP (syns, syn-acks, acks, fins, fragments)
        b. UDP (random port floods, fragments)
        c. ICMP (unreachable, echo, fragments)
        d. DNS
    2. Client Attacks
        a. Inactive and total connections
        b. HTTP Get flood

3. BGP attacks

ROSI calculations for the risk

Cost of Cisco Solution set: The cost of the system is defined on prorata basis and particularly to customer's use cases. Cisco systems prefers to offer a quote to the customers after consulting them personally and understanding their needs and demands. With the limited data available online, we were able to get an estimated range of cost of installation of these systems. The cost for implementing those solution are range $135.000 - $200.000 [10]

$$ROSI = \frac{(risk\ exposure \cdot \%risk\ mitigated) - solution\ cost}{solution\ cost}$$

Income:

Cost to customer = $10 per month

cost to customer per year = $120

Number of clients/customers = 20,000

Net Income = $2,400,000

Cost:

Fixed and Variable expenses of company = **$1,500,000**

Investments:

1. estimated cost to gain a new customer = $9-$20

   Through advertisements, campaigns, etc. If we lose rapport in the market then our investments to gain new customers are lost.

Potential loss in case of DDoS:

1. Loss of performance = **estimated 70%**
   a. DDoS triggered from our servers by spoofing our IPs would lead to reduced performance
   b. this translates to an estimated loss of 40% of utilized revenue ,i.e, 70% of $900,000 = **$630,000 (risk exposure)**
2. Bad Rapport Loss = 10% of cost to gain new customers
   a. assuming we have 1000 new customers per year, we lose **$9000-$20,000**

Net Loss= $650,000

Solution costs:

1. Investment on CISCO system = **$135,000 - $200,000** one time cost

   Based on the claims from reviews of devices, we assume that with this implementation the risk reduces by 75%.

$$ROSI = \frac{(650.000 \cdot 75\%) - 200.000}{200.000} \simeq \mathbf{144\%}$$

Hence, with the investment in the discussed risk strategy, our return on investment would be **144%.**

7. Conclusion

This introductory paper presents the basis of Return on Security Investment calculation and how it can help many DDoS victims (individual or organization being attacked.) in assessing their cost effectiveness. ROSI is a complex topic and this first attempt to introduce this topic has to be further developed to address remaining issues on DDoS and ROSI calculation:

1. Which model best applies to DDoS victims ?
2. What to include in the cost of an incident?
3. How to measure the added value of DDoS victim teams in incident handling?
4. Most importantly annualized losses without the solution?

Some of the direct cost were also hard to find but then indirect costs has too many factor so it’s hard to get the proper losses earlier as well as the cost.

As part of this work, the calculations performed are is addressing the topic of cost of incidents and return on security investment. The results of this research will help DDoS victims in assessing their profitability.

DDoS attacks will continue to grow in scale and severity thanks to increasingly powerful (and readily available) attack tools, the multiple points of vulnerability of the Internet, and business' increasing dependence on the Internet. As the cost of these attacks rise, providers, enterprises, and governments must respond to protect their investments, revenue, and services.

What is required is a new type of solution that complements existing security solutions such as firewalls and IDSs by not only detecting the most sophisticated DDoS attacks, but also delivering the ability to block increasingly complex and difficult-to-detect attack traffic without impacting legitimate business transactions. Such an approach demands more granular inspection and analysis of attack traffic than today's solutions can provide.

8. RÉFÉRENCES

[1] ISO 27001 and risk assessments:
http://www.itgovernanceusa.com/risk_assessments.aspx
[2] Spoofer Tool: http://spoofer.caida.org/summary.php
[3] Introduction to Security and Network Forensics By William J. Buchanan, (CRC Press, 6 June,2011), *[page 13, Figure 1.9]*
[4]Introduction to Security and Network Forensics By William J. Buchanan, (CRC Press, 6 June,2011)
[5] A Practical Introduction to Security and Risk Management By Bruce Newsome (SAGE Publications, 15 Oct 2013)
[6]http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html
[7]http://www.networkworld.com/article/2333552/lan-wan/cisco-details-strategy-for-catalyst-firewall-services-module-and-anti-ddos-gear.html
[8]http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/product_data_sheet0900aecd800fa552.html
[9]http://www.cisco.com/c/en/us/products/collateral/security/guard-xt-5650a/product_data_sheet0900aecd800fa55e.html
[10]http://itprice.com/cisco-gpl/AGX&sa=D&ust=1476698467133000&usg=AFQjCNGXkFmNufyk2XP4eBzW1jTUaPQDYQ