Cent. Eur. J. Comp. Sci. • 1(3) • 2011 • 355-366
DOI: 10.2478/s13537-011-0024-y

VERSITA

Central European Journal of **Computer Science**

Taxonomy of DoS Attacks and Their Countermeasures

Review Article

Simona Ramanauskaite[1*], Antanas Cenys[2†]

1 *Department of Information Technology, Siauliai University, Vilniaus st. 141, LT-76353 Siauliai, Lithuania*

2 *Department of Information Systems, Vilnius Gediminas Technical University, Sauletekio st. 11, LT-10223 Vilnius, Lithuania*

Received 22 January 2011; accepted 7 September 2011

Abstract: DoS attacks can vary in type, depending on many different criteria, as well as their countermeasures. Detailed taxonomy can help distinguish all possible types and be used for better understanding of the situation. This study reviews existing DoS attack and DoS attack countermeasure classifications and offers new classification schemes. The proposed DoS attack taxonomy has a new attack characteristic, which describes how bug exploitation can be used for DoS attack execution, as well as new possible values for resource depletion attack and the ways of agent army formation. We also clarify methods for DoS effect achievement and position them in the DoS taxonomy hierarchy. While for DoS attack countermeasure taxonomy we combine ideas from existing taxonomies and compose a three criteria hierarchy with average detailing level. All criteria and categories are described, and seven DoS attack and seven DoS attack countermeasure taxonomies are analysed to obtain their characteristics. Some research is also done to show their application capabilities.

Keywords: DoS • Denial of Service • countermeasure • taxonomy

© *Versita sp. z o.o.*

1. Introduction

Nowadays some Internet services have become critically important. Therefore degradation of service quality or total denial of service can be crucial. A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users.

The direct goal of DoS attacks is to deny some kind of service for a certain time period. This also leads to the other consequences: harm to the reputation of company, customer and financial loses, and in the vital service cases even has an impact on human lives.

Distributed denial of service (DDoS) attack is a cyber attack where multiple compromised systems (which are usually infected by malicious code) are used to target the single system causing a DoS effect on it.

* *E-mail: simram@it.su.lt*
† *E-mail: antanas.cenys@fm.vgtu.lt*

Securelist notes, that "According to the bookmakers, a few hours of website downtime can result in the loss of significant sums – 25-40,000 euros for large offices and 5-6,000 euros for smaller offices" [11]. According to Shadowserver Foundation data [13], there were 13757 unique DDoS targets in 2010. These numbers do not reflect all DoS and DDoS scale because they are related to only direct damage cases and can be even bigger in real situations.

The variety of DoS and DDoS attacks is one of the reasons why it is hard to fight against them. Clear DoS attack classification allows describing all types of attacks considering their properties.

There are many ways to consider the DDoS classification and many different taxonomies exist: D. Karig and R. Lee [7] classify DoS attacks considering the place where the attack strikes (network device, operating system, application, data or protocol); A. Fadlallah and A. Serhrouchni [4] first of all suggest to distinguish one source (DoS) attacks and multi source (DDoS) attacks; S. Specht and R. Lee [12] differentiate attacks by the resource they are exhausting and possible characteristics in these categories.

Later characterizations are more multidimensional. C. Douligeris and A. Mitrokotsa [5] consider four dimensions for attack classification (automation degree, vulnerability exploitation, attack rate dynamics and impact on victim) while J. Mirkovic and P. Reiher [9] add four more (source address validity, possibility of characterization, persistence of agent set and victim type).

The hierarchical classifications do not represent the full view of DoS attacks, while some existing multidimensional taxonomies can be very detailed and difficult to use for non-experts because of insufficient knowledge.

We propose a new multidimensional DoS attack taxonomy and add a new attack characteristic, which describes how bug exploitation can be used for DoS attack execution, as well as new possible values for resource depletion attack, the ways of agent army formation. We also clarify methods for DoS effect achievement and position them in the DoS taxonomy hierarchy.

As well as DoS attacks, their countermeasure taxonomies can be used for better situation analysis, too. D. Kagir and R. Lee [7] categorise countermeasures by victim type with minimal classifications in these groups, while A. Asosheh and N. Ramezani [1] use types of victim according to countermeasure phase (prevention or detection) and detail it more specifically. D. Champagne and R. Lee [3] suggest mitigation as one more phase while C. Douligeris and A. Mitrokotsa [5] distinguish response phase, too. The biggest number of countermeasure phases is represented in S.M. Specht and R. Lee [12] taxonomy. There are six phases, such as: detection and neutralization of handlers; detection and prevention of secondary victims; detection and prevention of potential attacks; mitigation and stopping of attacks; deflection of attacks; post-attack forensics.

The DDoS countermeasure taxonomy of C. Douligeris and A. Mitrokotsa [5] besides countermeasure phases, distinguishes one more dimension – location of countermeasure. Other multidimensional DDoS attack countermeasure classifications are proposed by A. Fadlallah and A. Serhrouchni [4] and J. Mirkovic and P. Reiher [9] taxonomies where along with countermeasure phase and its location they add degree of cooperation. Such multidimensional classifications allow characterizing the countermeasure in greater detail.

In our proposed DoS attack countermeasure taxonomy we also use three dimensions and try to categorize them without any connection to specific existing countermeasures. Therefore the classification criteria are detailed but with some level of abstraction, allowing the usage of this taxonomy for not yet existing countermeasures, too.

The aim of this work is to create more universal and easier to apply taxonomies for DoS attacks and their countermeasures, and analyse its usage in practice with non-professionals who have basic knowledge of DoS attacks ant their countermeasures.

The work is divided into five sections. In the next section, a new DoS attack classification is proposed and described, while Section 3 proposes and describes a new scheme for DoS attack countermeasure classification. In Section 4 we introduce the results of DoS attack and their countermeasure taxonomies statistical analysis, as well as results of research based on the application of these taxonomies. The last section summarizes the work and presents the final conclusions.

2. The proposed DoS attack classification

All attacks seek to make influence on some kind of victim. But DoS attacks differ depending on what kind of weakness is demonstrated by the victim. S. Specht [12] separates bandwidth and resource depletion groups. For full description of the exploited weakness, there also has to be a bug exploitation category, mentioned in F. Kargl's paper "Protecting Web

Servers from Distributed Denial of Service Attacks" [8]. We take it into account and classify DoS attacks considering vulnerability exploitation into these categories:

- **Bug exploitation attack.** Sometimes there are bugs in the victim's technical equipment or software that can be used to attack the victim. If the attacker uses the bugs existing in the victim's system for its denial from the service, such an attack falls into the bug exploitation attack category. This category can be split into subcategories:
  - *Attack from outside.* If exploitation of a bug existing in the victim's system directly affects the desired service, this kind of attack is called the attack from outside.
  - *Attack from inside.* Sometimes the attacker knows that there is a bug in the victim's system, but this bug is in some other service, and not in the one which he wants to deny. If the attacker exploits a bug in the victim's system to get some kind of system control and then uses that control to affect the desired service, this attack falls into the attack from inside category (service is denied from the same system where it is located).

- **Resource depletion attack.** When a system receives a query, it allocates the relevant part of its resources to the query processing and possibly its execution. If all queries require quite a lot of resources, there could be not enough resources in this system for all incoming queries and it stops working properly. The resource depletion attack uses such situations for denial of service.

  Considering the exhausted resource type, this type of attack may be divided into these subcategories:
  - *Memory depletion attack.* Some systems for all incoming queries allocate a certain amount of memory, which is limited. If the attacker manages to createa situation where all available memory is allocated for queries and there is not enough memory for the new ones, this service is denied by the memory depletion attack.
  - *CPU (Central Processing Unit) work depletion attack.* Usually incoming data is processed in one way or another. Sometimes it requires quite a lot of CPU work. If the attacker manages to supply incoming data which requires even more CPU work to analyze or process this query, CPU may give excessive attention to this one job and be unable to do other jobs. If such a situation leads to denial of service, it can be described as CPU work depletion attack.

  Resource depletion attacks may be classified into subcategories by attack packet modification necessity:
  - *Brute-force resource depletion attack.* An attack where sufficiently huge number of incoming queries denies a service is called a brute-force resource depletion attack. There is no need for the attacker to modify attack packets. A huge amount of data is enough to reach the goal.
  - *Semantic resource depletion attack.* Some systems use more resources if incoming packets are modified. In such cases there is no need for huge amount of incoming data to deny the service. If a service is denied because of modified incoming data influenced resource depletion, this kind of attack falls into the semantic resource depletion attack category.

- **Bandwidth exhaustion attack.** Bombarding target with a huge amount of data, the situation can be created where there is no more opportunity to send other data to the victim because of bandwidth exhaustion. Such a situation is called bandwidth exhaustion DoS attack.

Another property, because of which DoS attacks can vary, is the attacker size. It is important how many packets the attacker can generate for its target within a certain period of time. However, it is more important to know what you are fighting with: if it is one computer or many coordinated for one attack.
Like A. Fadlallah [4], we also clearly distinguish the difference between single source and multiple source DoS attack:

- **Single source attack.** If the attack is launched from a single attacking machine, it is called a single source attack. Usually it is the attack of bug exploitation or semantic resource depletion attack groups or extremely powerful machines able to reach flood attack success.

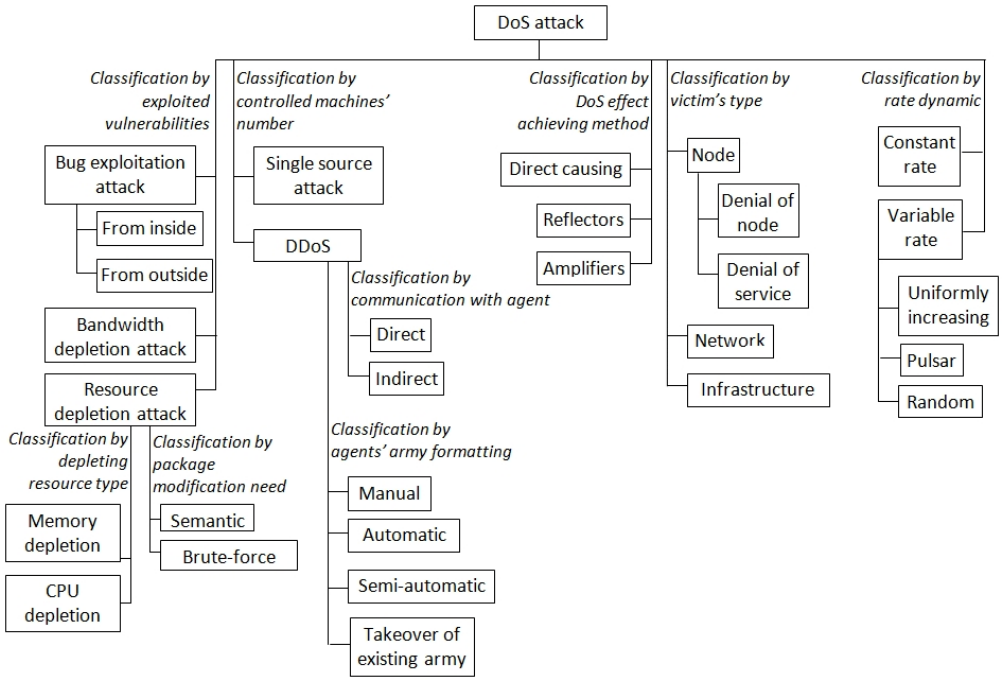


Figure 1. Proposed DoS attack classification scheme.

- **Distributed Denial of Service (multiple sources) attack.** Before launching an attack, the attacker sets up an attack network (Botnet). They control the network and use it for one big and coordinated attack. Such a coordinated attack from multiple sources is called a distributed denial of service attack.

  In many DDoS classifications, there is one group for attack automation description [5, 9]. We propose to distinguish agents' (also named zombies or slaves) army formation and its management phases. In order to form the agent army attacker, it is necessary to find vulnerable machines and to install malicious code necessary to control that agent. Depending on automation of this action, agent army formation can be divided into four categories:

  – *Manual agent army formation.* When the attacker has to find vulnerable machines and install malicious code into them himself, this way of agent army formation is called manual.

  – *Semi-automatic agent army formation.* Sometimes the attacker uses various tools for finding vulnerable machines and installing malicious code into them or uses tools just for one of these stages and the other installation is done manually. Such an agent army formation strategy is called semi-automatic because in some situations it requires human attention.

  – *Automatic agent army formation.* Automatic agent army formation requires human action just to launch the tool which will do all necessary tasks to form the agent army.

  – *Takeover of an existing agent army.* There are agent armies which can be borrowed, rented or even stolen (taken over management). Takeover of the existing agent army does not require finding vulnerable machines, but concentrates on finding an existing agent army and gaining control over it.

A vulnerable machine becomes an agent when it runs malicious code which ensures that the agent will be able to execute an attack (enforcement function), and the handler will be able to control that agent (communication function) and sometimes code for the discovery of other agents (spread function).
A. Asosheh [1] classifies DDoS attack tools into Agent-based (Agent Handler and Reflector) and IRC-based. It represents the idea of communication between agents and the organizer of the attack. On this basis, we make categories considering how the communication with agents can be implemented:

- **Direct command assignment.** After turning into an agent, some machines stop listening on certain ports because all instructions and information is transmitted to these agents through these ports. The situation is called direct command assignment, because commands are transmitted directly to such an agent.

- **Indirect command assignment.** Indirect communication can be implemented e.g., using IRC (Internet Relay Chat). After becoming an agent, the machine goes to the appropriate chat room and monitors the ongoing conversation. Commands are transmitted into that chat, but not directly to the agent, so it is called indirect command assignment.

Usually an attacker uses stepping stones, proxy servers and other ways to hide his existence and decrease the probability of being traced back after identifying attack agents (direct communication with agent would simplify the traceability, because of smaller amount of data to be analysed to identify the attacker). However, there are methods which look like masking techniques but are intended to increase DoS effect (by increasing the amount of traffic or by circumvention of security measures).
Different authors classify these methods as a data flood depletion attack [12], a type of structured attack [4], a subcategory of vulnerability exploitation attack [12], or a data flood attack [7]. We make these methods separate as the new property of DoS attack, i.e. methods for achieving DoS effect:

- **Direct causing of DoS effect.** If the attack traffic from the agent is transmitted directly to the target of the attack, this method is called direct.

- **Reflector usage.** Sometimes the attack traffic is transmitted not to the direct target, but to an intermediate machine. This machine reflects the received traffic not to the original sender but to the real target. Usually it is achieved by spoofing attack packets and is called reflector usage.

- **Amplifier usage.** If attack packets indicate the IP address of the target as the broadcast address, these packets will be retransmitted to all machines on the given subnet. Such an opportunity lets the attacker to amplify the attack and facilitates the achievement of the DoS effect. This method is called amplifier usage and is used to attack no only individual machines, but even whole networks.

D. Karig [7] distinguishes five types of victims in DoS attacks. We separate three categories for clarification of the real objects and in order not to overwrite already existing categories:

- **Node.** Target type is node if the attack is targeted just on one Internet node and directly does not affect the work of other nodes.

  The impact on the node can vary. Respectively, we distinguish two types of target nodes:

  - *Denial of node.* If the attacker tries to deny service by denying a node (this node do not respond at all or shuts down), this kind of target is treated as all node.
  - *Denial of service in a node.* If the attacker denies one or few services in a node, but this node can continue other services the attack target is service in a node.

- **Network.** If the attacker wants to deny service for a certain network or make the network act up, the attack target is the network.

- **Infrastructure.** There are distributed services, which can be denied by denying just one or few nodes in its structure. The Internet and DNS importance in this infrastructure is one of the examples. If the attacker is targeted at denying of something what can deny the distributed system, this attack target is not just a node but the infrastructure.

The attack's dynamics is also important for describing DoS attacks, because of the possibility to detect an ongoing attack at the early stages. There can be two main categories for attack rate description:

- **Constant rate.** Attacks where agent machines generate attack packets at a steady rate (usually as many as their resources permit) are called constant rate attacks.

- **Variable rate.** Variable rate attacks vary the attack rate of an agent machine in order to delay or avoid detection and response. Usually authors describe increasing and fluctuating attack rate dynamics [5, 9]. We specify three possibilities:
  - *Uniformly increasing.* If the attack rate increases with time by a certain rate, this attack is called uniformly increasing. This way, the victim's resources can be slowly exhausted without being noticing the attack.
  - *Pulsar.* The attack is called pulsar if its rate increases and then decreases from time to time. Changes are because of the victim behaviour or preprogrammed timing, occasionally relieving the effect to avoid detection.
  - *Random.* To avoid attack detection, the attacker tries to generate as much random packets as possible. Such attacks are called random.

All distinguished DoS attack properties and categories form a certain DoS attack classification (see Figure 1). The information about an attack has to be indicated in all five categories in order to fully describe the DoS attack.

3. The proposed DoS attack countermeasure classification

The main criteria for DoS countermeasure classification are the phase of actions in the attack process. According to the criteria, we separate these categories:

- **Prevention.** Prevention tries to block a DoS attack before it actually happens or adequately prepare for future attacks. Like J. Mirkovic [10], we divide the prevention phase into:
  - *DoS prevention.* DoS prevention includes all measures necessary to avoid the DoS effect but not an attack. These measures can be divided into resource management, elimination of vulnerabilities and deflection. We suggest to describe it in a more detailed way:
    - *Resource multiplication.* Resource multiplication means adding additional resources to be sufficient to cope with an incoming attack.
    - *Resource accounting.* If resources are restricted for non-privileged users, the prevention mechanism is called resource accounting. Examples of such a mechanisms can be client puzzles [6], or cost-functions [2].
    - *Patches and upgrades.* All systems must be up to date, and the necessary update process is called prevention (regular patches and upgrades).
    - *Built-in defences.* There are vulnerabilities which cannot be eliminated by means of patches or upgrades and require additional help. Built-in defences are another way to prevent system vulnerabilities exploitations.
    - *Deflection.* Honeypots are systems with limited security that can be used for traffic and analysis of its characteristics by deflecting the potential attack traffic.
  - *Attack prevention.* Unlike DoS prevention, attack prevention tries to prevent the possibility of DoS attack, no matter what kind. This kind of prevention measures concentrate on the global networks maintenance, and not only the machine. Similarly to M. Specht [12], we classify four possible ways of attack prevention:
    - *Detect and neutralize handlers.* If we would detect all the existing handlers, there would be no possibility to execute a DDoS attack managed by the handler-agent architecture.
    - *Detect/Prevent secondary victim.* Agents are innocent machines whose control is taken over by the attacker. Detecting all the vulnerable machines and preventing them from being taken over would stop the DDoS attack possibility.
    - *Detect/Prevent potential attacks.* Monitoring the Internet traffic, it is possible to observe signs of attack. It can be done using egress filtering and MIB statistics.
    - *Dynamic pricing.* If network service providers would take taxes for the network usage, all machines would be more interested in prevention, i.e. that they would not be improperly used. This way, sometimes the price of desired flooding attack can become bigger in comparison to the benefit of the attacker.

- **Detection.** If prevention was not sufficient, it is very important to detect an incoming attack as soon as possible. For attack detection, there are a couple of information sources. Considering the observed attack detection information, detection measures can be divided into three categories:

  – *Packet header observation.* Packet header observation includes the IP address and other packet attributes supervision.

  – *Packet content observation.* If packet content is observed to identify a DoS attack, this kind of detection mechanism is called packet content observation.

  – *Traffic rate observation.* According to the incoming traffic rate, it is possible to indicate the incoming DoS attack. In such a case, the detection mechanism is called traffic rate observation.

  The other criteria used to classify detection phase are related to strategies used to detect the attack. We consider J. Mirkovic's [10] reactive level DDoS defence mechanisms classification and separate three groups:

  – *Pattern detection.* The strategy based on the comparison of all communications with the existing records in the attack signatures database is called pattern detection.

  – *Anomaly detection.* Anomaly detection strategy tries to compare normal traffic with the incoming traffic, and alerts if the traffic is too different from normal.

  – *Third-party detection.* Mechanisms that deploy third-party detection and do not handle the detection process themselves, but rely on external systems.

- **Mitigation/Stop.** The mitigation phase tries to lighten or even stop the attack. Instead of very detail mitigation classification as in D. Champagne and R. Lee [3] taxonomy, we prepare more abstract one, as proposed by M. Specht [12], which is oriented to more universal countermeasures (meant for all types of DDoS attack mitigation but not specific victim type):

  – *Load balancing.* Load balance means bandwidth, memory or other victim's resource increase on critical situations or even server replication.

  – *Flow control.* The max-min fair server-centric router throttle method sets up routers that access the server with logic to adjust (throttle) incoming traffic to the level that will be safe for the server to process. Flow control can be used for application level too, using different software or hardware solutions.

  – *Drop request.* To mitigate an attack some requests can be randomly or specifically dropped.

- **Post-action forensics.** All attacks must be suitably analyzed to prevent similar situations in the future. C. Douligeris [5] calls it the intrusion response and describes such an internal classification, so do we:

  – *Traffic pattern analysis.* During a DoS attack, traffic pattern data can be stored and then analyzed. It allows updating the information for later attack detection or even mitigation.

  – *Analysis of event logs.* Analysis of event logs, selected from the attack period, allows to more specifically determine the type of attack and to prepare for such attacks if they happen again.

  – *IP trace back.* In order to determine and possibly eliminate the attacker, it is important to trace back the attack traffic.

The other criterion for DoS countermeasure classification is countermeasure location. C. Douligeris, A. Fadlallah and J. Mirkovic [4, 5, 10] separate three possible places. We suggest four possible locations:

- **Victim machine.** Some DoS attack countermeasures are designed to be used on a single machine, to defend it against an attack or at least to mitigate it.

- **Victim network.** If a countermeasure should save all computers in a network from the DoS effect or even self attack, it has to be deployed in the victim's network.

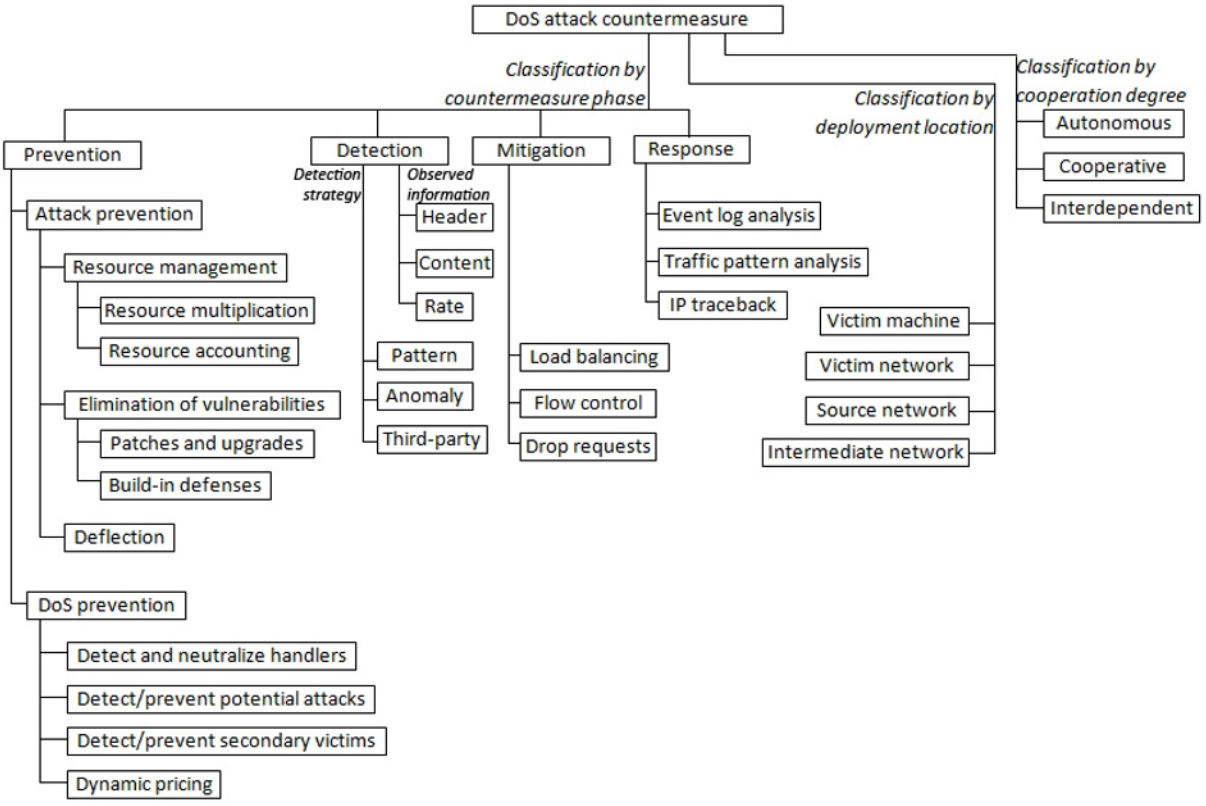


Figure 2. DoS countermeasure classification scheme.

- **Source network.** The DoS countermeasure deployed in the same network as the attacker and meant to block all the outgoing attack traffic is called defence in source network.
- **Intermediate network.** Intermediate network countermeasures should ensure defence to a large number of hosts. It should be deployed somewhere in the Internet and monitor all suspicious traffic.

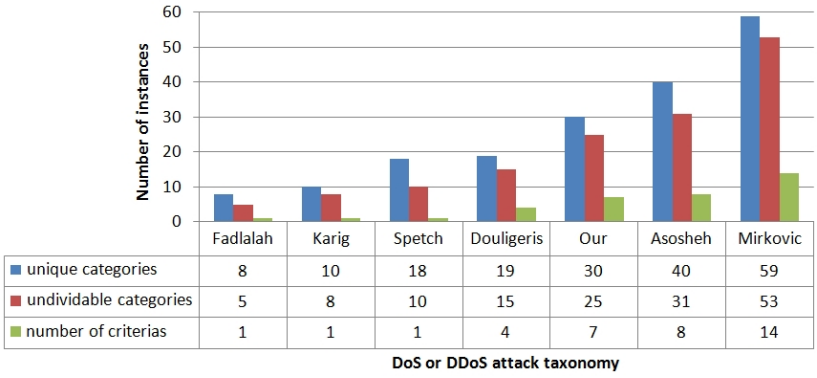
One more topic criterion for DoS countermeasure classification is the cooperation degree, mentioned in A. Fadlallah and J. Mirkovic's [4, 10] works. It allows estimation of the attacker type, and we distinguish three possible cases:

- **Autonomous.** Autonomous mechanisms perform independently at the point where they are deployed (a host or a network).
- **Cooperative.** Cooperative mechanisms usually cooperate with the other systems, but also can work autonomously.
- **Interdependent.** Interdependent mechanisms cannot operate autonomously at the single deployment point. They require deployment at multiple points.

All distinguished DoS attack countermeasure properties and categories form a certain DoS attack countermeasure classification (see Figure 2). Information about the attack has to be indicated in all three categories attempting to fully describe a DoS attack countermeasure. Because of distributed and composed protection, there is a possibility to distinguish one countermeasure even considering a couple of categories.

4. Comparison of DoS and their countermeasure taxonomies

We analysed existing DoS attack and their countermeasure taxonomies by numbers: how many categories are represented in the taxonomy (overall and those which are not divided into smaller ones) and how many classification criteria



	Fadlalah	Karig	Spetch	Douligeris	Our	Asosheh	Mirkovic
unique categories	8	10	18	19	30	40	59
undividable categories	5	8	10	15	25	31	53
number of criterias	1	1	1	4	7	8	14

Figure 3. Statistical data for analysed DoS attack taxonomies.

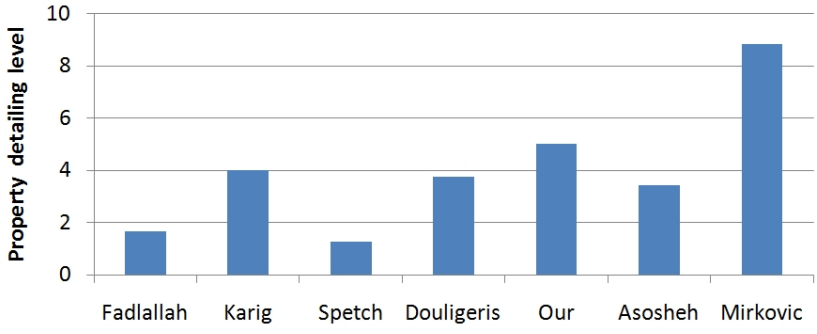
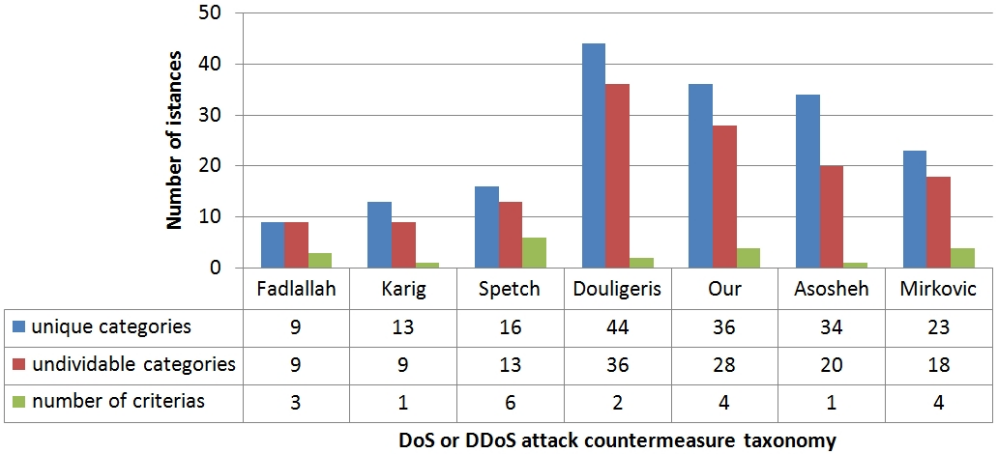


Figure 4. Category detailing level for analysed DoS attack taxonomies.

(dimensions) are used in the taxonomy.
For this analysis we used seven DoS and its countermeasure taxonomies of the following authors:

- A. Asosheh and N. Ranezani [1];
- C. Douligeris and A. Mitrokotsa [5];
- A. Fadlallah and A. Serhrouchni [4];
- D. Karig and R. Lee [7];
- J. Mirkovic and P. Reiher [9];
- S. M. Specht and R. Lee [12];
- Our proposed taxonomies.

The analysis of DoS or DDoS taxonomies showed that all these taxonomies have different level of detailing, which in DoS attack classifications varies from 1 dimension, 5 undividable and 8 unique categories per taxonomy to 14 dimensions (different level), 52 undividable and 59 unique categories per taxonomy (see Figure 3).
For estimating the property detailing level, we consider the number of undividable and divided into smaller groups categories. The level of property detailing showed that DoS taxonomy proposed by J. Mirkovic [9] have the biggest number of alternative values for the DoS attack property (see Figure 4).
Analysing DoS countermeasure taxonomies, there is no linear dependency between the number of categories and the number of criteria as in DoS taxonomies. Also, the numbers of categories and criteria are not as high as in DoS taxonomies (see Figure 5).



	Fadlallah	Karig	Spetch	Douligeris	Our	Asosheh	Mirkovic
unique categories	9	13	16	44	36	34	23
undividable categories	9	9	13	36	28	20	18
number of criterias	3	1	6	2	4	1	4

Figure 5. Statistical data for analysed DoS attack countermeasure taxonomies.

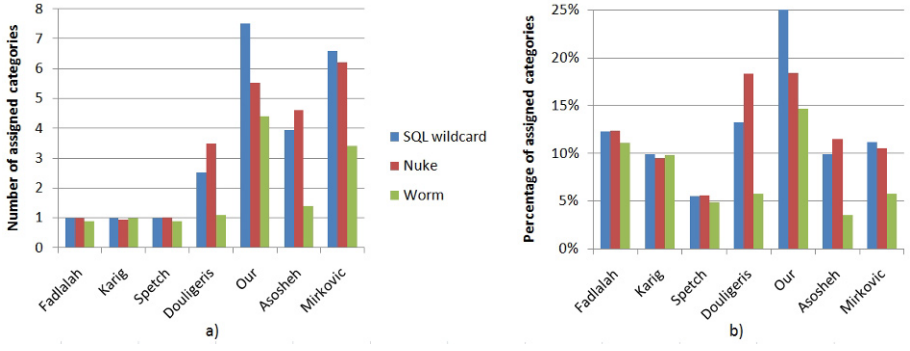


Figure 6. Number (a) and percentage (b) of assigned categories in certain DoS attack taxonomy for different type of DoS attack.

However, the presented statistics do not represent the application characteristics. Therefore we investigated the application of these taxonomies in practice - different DoS attacks were executed (SQL wildcard attack, Nuke attack and worm executed shutdown of specific service) to classify them according to analysed taxonomies. There were 34 respondents (Informatics engineering students) in the research and all of them classified the three different DoS attacks in all analysed taxonomies. They also suggested countermeasures for these attacks according to all analysed DoS countermeasure taxonomies.

One of these attacks could not be called a DDoS attack, because it happened because of one worm actions, while some of these taxonomies are meant for DDoS attack classification. However, this case allows us to judge if such an attack be classified by DDoS taxonomies or no.

The research results showed that classifying SQL wildcard and worm attacks the students marked the biggest number of categories in our proposed taxonomy. While the biggest number of Nuke attack categories were marked in the J. Mirkovic's [9] taxonomy. However, estimating the proportion between marked and existing categories in the taxonomies, the results differ and just prove the usage simplicity of our proposed DoS attack taxonomy (see Figure 6).

Analysing the DoS countermeasure suggestions for a specific DoS attack, the biggest number of proposed countermeasures was in our proposed taxonomy. However estimating the percentage between number of possible categories and suggested countermeasure categories, the biggest percentage of taxonomy categories was proposed in A. Fadlallah [4] and J. Mirkovic [9] proposed taxonomies (see Figure 7).

The experiments showed that the taxonomies proposed in this paper are easiest to apply, while non-traditional DDoS attack classification in different taxonomies can have fewer properties than the traditional ones. In the case of DoS

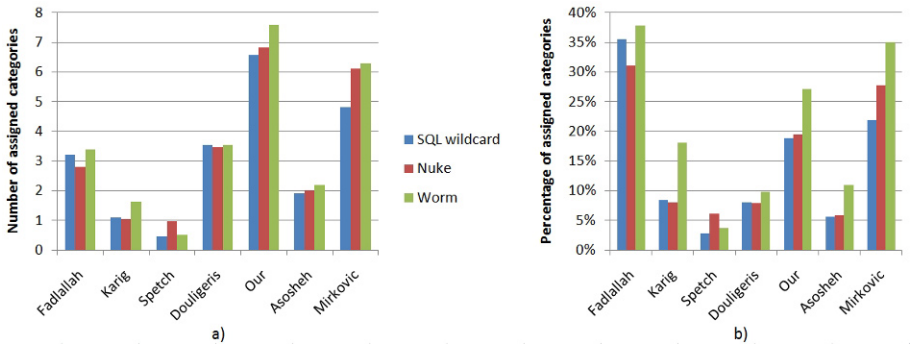


Figure 7. Number (a) and percentage (b) of proposed categories in certain DoS attack countermeasure taxonomy for different types of DoS attacks.

attack countermeasure taxonomies for the worm type attack, the interrogated students had more suitable categories to suggest than for traditional DDoS attacks.

5. Conclusions

The review of the existing DoS attack and their countermeasure classifications showed that all of them are very different. We took the useful ideas from existing taxonomies and proposed more detailed and universal taxonomies for DoS attack and DoS attack countermeasure.

The taxonomies proposed in this paper are suitable to describe DoS attacks and their countermeasures from different perspectives: attacker, victim, researcher, i.e. the taxonomies are universal to use. It was achieved by selecting the most important criteria and not associating them only with the user group (properties, important and known only by the attacker or another group are not included), which allows these classifications to be one of the easiest to use for non-professional DoS attack specialists.

All separated criteria and categories of the proposed taxonomies were briefly described. This approach enables unambiguous and unique description of all possible cases considering these classifications and gives basis for a common terminology for researchers working on DoS attacks and their countermeasures.

The statistical characteristics of DoS attacks and their countermeasure taxonomies such as the number of criteria, unique and undividable categories do not reflect the taxonomy application characteristics. More detailed research should be done to estimate the application areas for a specific taxonomy to get all the best it can offer. Our proposed DoS attack taxonomy is one of the easiest to apply for persons with basic DoS attack knowledge. Although the usage of our proposed DoS attack countermeasure could be better, it also seems to perform as well as other compared taxonomies.

References

[1] Asosheh A., Ramezani N., A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification. WSEAS Transactions on Computers, 2008, 7, 281-290

[2] Back A., Hashcash - a denial of service counter-measure, 2002, 1-10, http://www.cypherspace.org/hashcash/hashcash.pdf

[3] Champagne, D., Lee, R., Scope of DDoS countermeasures: taxonomy of proposed solutions and design goals for real-world deployment. In: 8th International Symposium on Systems and Information Security, 2006

[4] Fadlallah A., Serhrouchni A., Denial of service attack and schemes Analysis and Taxonomy, In: IEEE SETIT 2005, International Conference Sciences of Electronic, Technology of Information and Telecommunications (27-31 Mar. 2005, Tunisia), 2005

[5] Douligeris C., Mitrokotsa A., DDoS attacks and defense mechanisms: classification and state-of-the-art. COMPUT NETW, 2004, 44, 643-666

[6] Juels A., Brainard J., Client puzzles: A cryptographic countermeasure against connection depletion attacks. In: Proceedings of the 1999 ISOC Network and Distributed System Security Symposium, 1999, 151-165

[7] Karig D., Lee R., Remote Denial of Service Attacks and Countermeasures, Princeton University Department of Electrical Engineering Technical Report CEL2001-002, 2001

[8] Kargl F., Maier J., Weber M., Protecting Web Servers from Distributed Denial of Service Attacks. In: WWW10, Tent International World Wide Web Conference (1-5 May 2001, Hong Kong), ACM, 514-524, 2001

[9] Mirkovic J., Reiher P., A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review, 2004, 34, 39-53

[10] Mirkovic J., Dietrich S., Dittrich D., Reiher P., Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall, 2005

[11] Namestnikov Y., DDoS attacks in Q2 2011, SecureList, 2011, http://www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011?print_mode=1

[12] Specht M. S., Lee R., Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In: 17th International Conference on Parallel and Distributed Computing Systems, 2004, 543-550

[13] Shadowserver Foundation, DDoS Historical, 2011, http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSHistorical