World Applied Sciences Journal 25 (3): 404-409, 2013
ISSN 1818-4952
© IDOSI Publications, 2013
DOI: 10.5829/idosi.wasj.2013.25.03.13317

Denial of Service in Components of Information Telecommunication Systems Through the Example of “Network Storm” Attacks

Alexander Grigorievich Ostapenko, Sergei Sergeyevich Kulikov,
Nikolai Nikolaevich Tolstykh,
Yuri Gennadievich Pasternak and Larisa Georgievna Popova

Voronezh State Technical University, Voronezh, Russia

Submitted: Aug 21, 2013; **Accepted:** Sep 28, 2013; **Published:** Oct 3, 2013

Abstract: The article is dedicated to the study of “network storm” attacks aimed at disrupting the availability of information and information resources. The author has examined scenarios and models for “network storm” attacks, which exploit the vulnerability of the hardware and information technology of attacked components of information telecommunication systems (ITCS). The first scenario implies exploiting a vulnerability during the switching process – flooding a switch’s MAC Table through a massive MAC flooding attack, whereby a malicious user can direct a critical volume of malicious traffic at all the elements of an ITCS being attacked, which will result in a denial-of-service and lead to a disruption of the availability of information and information resources. Carrying out a “network storm” attack according to the second scenario implies exploiting a vulnerability during the routing process – when on the strength of the default settings there is a regular situation of uncertainty between two components of an ITCS, which can be exploited by the malicious user who directs a critical volume of malicious traffic at the elements of the ITCS being attacked, which will also lead to a disruption of the availability of information and information resources.

Key words: Information security • Information and telecommunication system • Network storm • Flooding attack • Denial of service

INTRODUCTION

Multiple studies reveal that attacks aimed at disrupting the availability of information and information resources rank high in frequency of occurrence, damage done and costs of protection against them [1-4].

A typical example of such attacks are “network storm” attacks directed at a an ITCS component (a structurally or functionally isolated part consisting of several elements), which consists of several elements (solitary hardware): computing and switching equipment.

It’s a complex comprehensive attack intended to force the switch of an attacked ITCS component to the ‘hub’ mode with a view to spreading critical volumes of legal and malicious onto the ITCS elements connected to the ITSC component’s switch (Figure 1).

When an attack of this kind occurs, the computing and switching function ITCS elements have to expend all of their resources on processing such traffic, which makes them inaccessible to ITCS users [5].

The “network storm” attack can be one- or two-staged. In the case of highly loaded ITCS’s [6], it’s just a matter of managing to cause the “unicast flooding” effect, whereby the entire traffic coming into the switch is passed along to all the elements connected to it. Incidentally, the whole critical volume of legal traffic will, in point of fact, become malicious. One can achieve this by implementing a MAC flooding attack, an STP attack, or using the ITCS’s routing vulnerabilities.

One can amplify the attack’s destructive impact by directing artificially generated malicious traffic at an attacked ITCS component. In this regard, there are several possible scenarios of implementing “network storm” attacks.

Corresponding author: Kulikov, Voronezh State Technical University, 394026, Voronezh, Moskovsky prospect, 14, Russia.

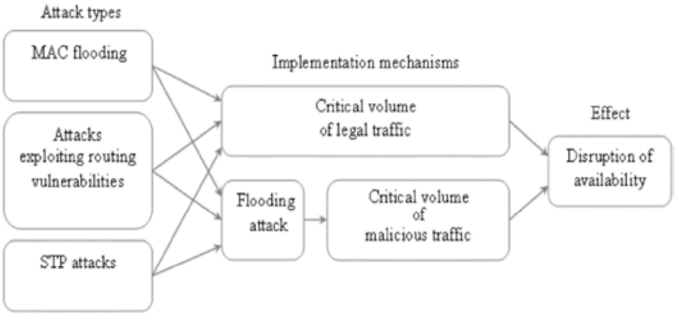
Attack types
MAC flooding
Attacks exploiting routing vulnerabilities
STP attacks
Implementation mechanisms
Critical volume of legal traffic
Flooding attack
Critical volume of malicious traffic
Effect
Disruption of availability

Fig. 1: Scenarios for the implementation of "network storm" attacks

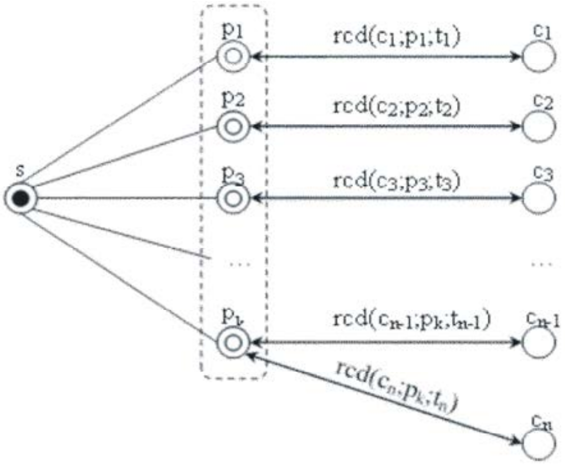

Fig. 2: The process of "teaching" the switch

Main Part: For storing the unique MAC addresses of devices whose sent network frames have reached a corresponding port, level-2 switches (s) use special system memory (Content Addressable Memory, CAM) [7]. CAM Tables, in point of fact, contain records (rcd) comparing the number of the switch port (p) to which a frame from the source came last with the MAC address of the frame's source (c). Note that information on this connection is complemented by a timestamp for its establishment (t). The process of filling and refreshing the switch's CAM Table is also called "teaching" about the ITCS structure (Figure 2).

The size of the CAM Table is limited; note that it can contain several thousand to several hundred thousand records simultaneously (R_{max}). In the event the malicious user (d) has access to the switch, he/she can cause the overfilling of the CAM Table by generating an avalanche-like flow ($m>>R_{max}$) of frames (frm) with fictitious MAC addresses, sending them through the attacked switch and, thus, creating lots of non-existent network devices (f), which will make it impossible for the network devices of legal ITCS users to interact with the attacked switch in the regular mode (Figure 3).

In order not to break the continuity of information processes in the ITCS, the attacked switch will, in point of fact, turn into a hub and will start redirecting all one-address flows going through it to all the ports, except the one to which the flow has come. As a result of this, the ITCS user equipment connected to the switch can fail (Figure 4). Furthermore, all the legal traffic will turn into malicious traffic whose critical volume will lead to a disruption of the availability of information and resources in the ITCS.

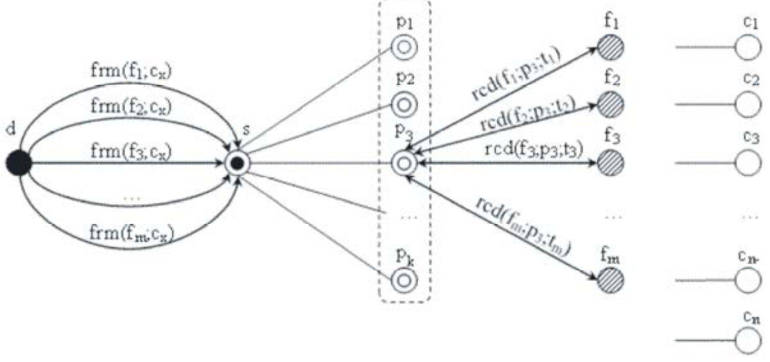

Fig. 3: The MAC flooding attack process

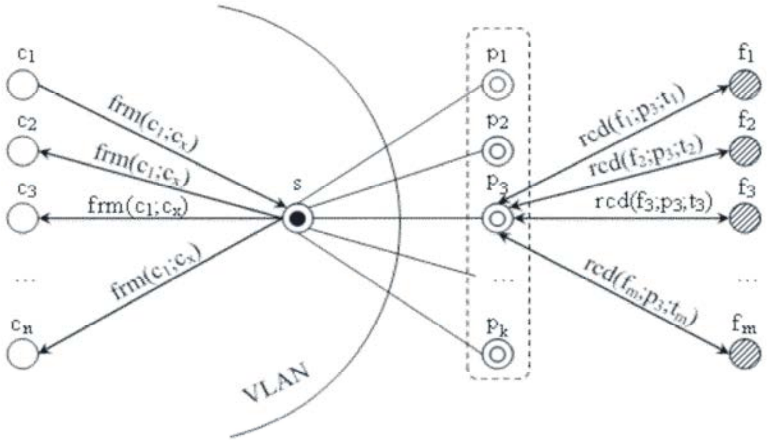

Fig. 4: The process of redirecting a one-address flow

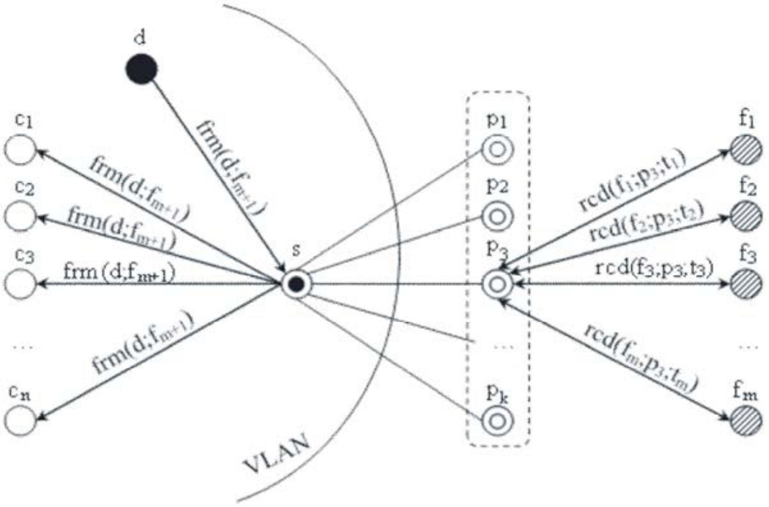

Fig. 5: The process of redirecting malicious traffic

If the malicious user has access to the ITCS's virtual component (VLAN) which belongs to the attacked switch, to amplify the effects of a "network storm" attack it is capable of (Figure 5) generating malicious traffic by itself too, effecting a flooding attack [8].

We'll now examine the scenario for a "network storm" attack, which is predicated on routing vulnerabilities. Let there be two virtual components of an ITCS, to each of which by default a level-3 switch is assigned as a gateway (s_1 and s_2). Here certain ITCS elements belonging to one virtual ITCS element are connected to the switch of the other virtual ITCS component. Let's assume that by a certain point in time, when an element of the first virtual ITCS component needed to get in touch with an element of the other virtual ITCS component, the IP addresses and MAC addresses of these elements were already present in the routing and switching tables of both switches (Figure 6).

After an ITCS element belonging to one virtual ITCS component sends a request to another ITCS element belonging to the other virtual ITCS component, respectively (Figure 7), the response can be expressed as, for instance, a UDP flow (Figure 8).

The aging and automatic cleanup of the switch's CAM Table occur by default every 5 minutes [9]. Thus, in 5-minute intervals, in case the default settings are used, the routers' CAM Tables will be shifting to a state generally depicted in Figure 9.

If any of the ITCS elements is trying again to get in touch with another element which is not from the same virtual ITCS component, in default of information on the receiver's MAC address in the CAM Table, the switch which is a gateway for the sender-element will redirect the packets received from the sender to all of its ports within a corresponding virtual ITCS component (Figure 10). The redirected

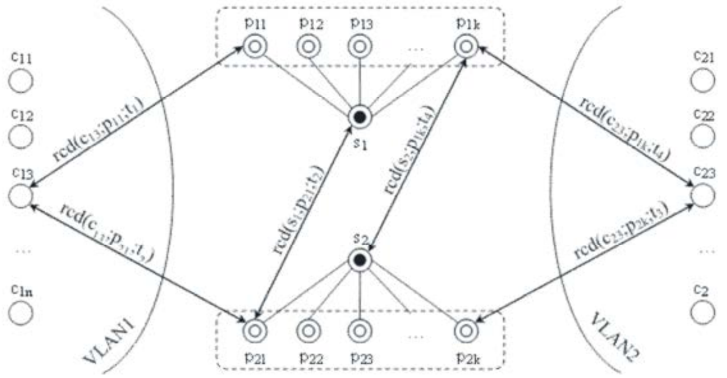

Fig. 6: The preliminary state of the routers' CAM Tables

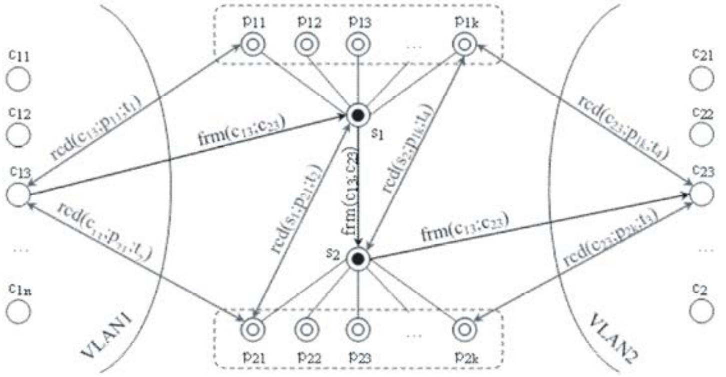

Fig. 7: The process of sending a request to an element that is a part of the other virtual component

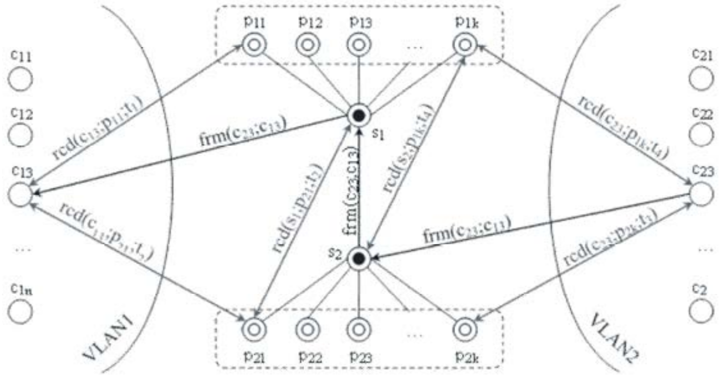

Fig. 8: The process of responding to a request of an element that is a part of the other virtual component

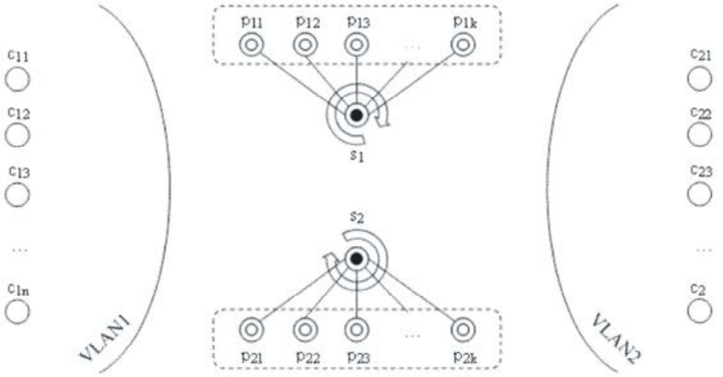

Fig. 9: The state of the switch CAM Tables after their aging

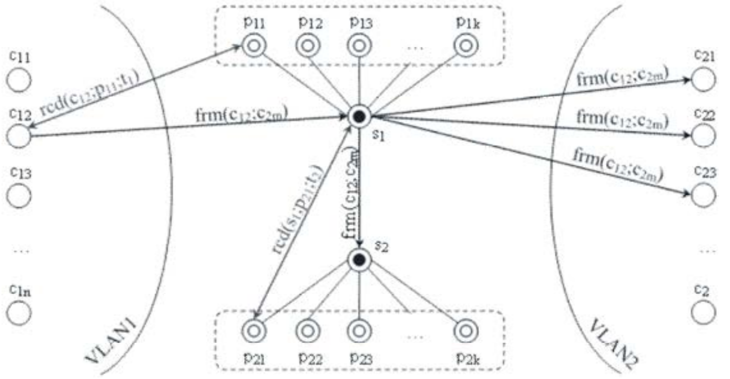

Fig. 10: The process of sending a request to the elements of a virtual component

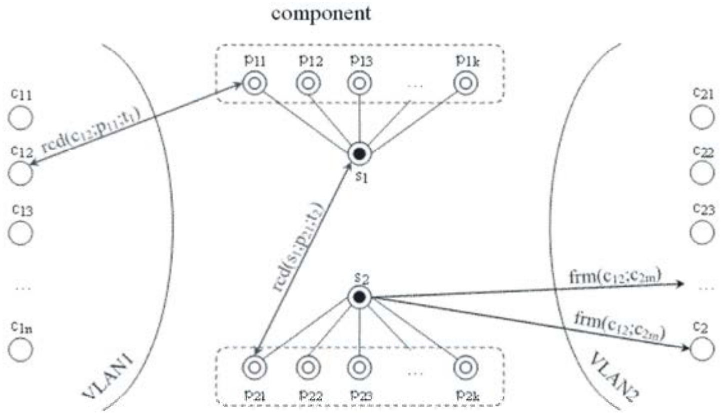

Fig. 11: The process of delivering a request to the sender element

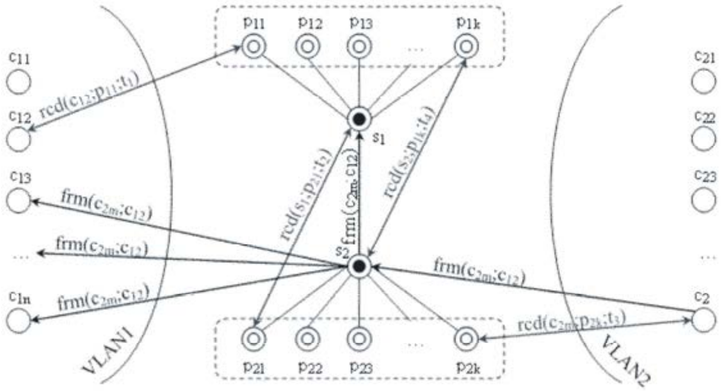

Fig. 12: The process of responding to a request of an element that is a part of the other virtual component

one-address flow, having gotten into the switch – the sender-element's gateway – will be delivered to the point of destination (Figure 11).

Responding to a request received, an ITCS element starts sending data to its gateway (e.g. a UDP flow [8]). But since a receiver-element's MAC address is not present in the router's CAM Table, the flow will be sent to all the elements of the ITCS which are a part of the receiver-element's virtual component of the ITCS (Figure 12).

As a result of such redirecting, ITCS elements will be receiving and processing critical volumes of traffic, which will lead to a disruption of the availability of information and information resources in the ITCS.

CONCLUSION

One of the simplest ways to perpetrate a denial-of-service attack (through the example of "network storm" attacks) is directing an avalanche-like flow of network packets at an attacked ITCS component whose switching and routing equipment has corresponding vulnerabilities. Processing such flows will engage most of the system's resources, which can make the attacked ITCS component inaccessible to legal user requests.

Hence, we can assert that attacks aimed at a disruption of the availability of information and information resources in ITCS's ("denial-of-service" attacks) can be implemented using different scenarios. The degree to which an ITCS is protected against such "service-of-denial" attacks can be assessed quantitatively using the mathematical and algorithmic apparatus of risk analysis [10-11].

Inferences: This study has yielded the following findings:

- The "network storm" attack has been defined as, in the first place, a complex comprehensive multi-staged attack that exploits various vulnerabilities of ITCS hardware and information technology.
- The study has examined scenarios and presented diagrams describing the implementation of "network storm" attacks, which exploit vulnerabilities in the process of switching between ITCS components and include the perpetration of a MAC flooding attack in the first stage, as well as exploit vulnerabilities in the process of routing between ITCS components.
- The findings obtained open up a prospect of building corresponding analytical risk models in designing diverse ITCS's that will be secured.

ACKNOWLEDGEMENTS

The article was written as part of one of Voronezh State Technical University's primary scientific research programs, *Managing Information Risks and Ensuring the Security of Info-communication Systems*; the authors extend their gratitude to the Department of Information Security Systems at the above university for help in preparing this publication.

REFERENCES

1. Moore, D., C. Shannon, D.J. Brown, G.M. Voelker and S. Savage, 2006. Inferring Internet Denial-of-Service Activity. ACM Transactions on Computer Systems, 24(2): 115-139.
2. Abliz, M., 2011. Internet Denial of Service Attacks and Defense Mechanisms. University of Pittsburgh Technical Report, No. TR-11-178.
3. Mirkovic, J. and P. Reiher, 2004. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, 34(2): 39-53.
4. Kulikov, S.S., 2013. An Investigation of Attributes of Vulnerabilities in Information and Telecommunication Systems / Kulikov S.S., Belonozhkin V.I. // Information and Security, 2: 255-256.
5. Ostapenko, G.A., 2012. Information Resources of Innovative Projects: Risk Modeling under Conditions of DDoS Attacks / Ostapenko G.A., Bursa M.V., Popov E.A., Vyakhireva S.S. // Information and Security, 3: 345-352.
6. High Availability Campus Network Design - Routed Access Layer using EIGRP, 2007. Cisco Press, pp: 103.
7. Froom, R., B. Sivasubramanian and E. Fahim, 2004. CCNP Self-Study: Building Cisco Multilayer Switched Networks (BCMSN), 2nd Edition. Cisco Press, pp: 816.
8. Junos, O.S., 2011. Security Configuration Guide, Juniper Networks, Inc., pp: 1774.
9. Campus 3.0 Virtual Switching System Design Guide, 2011. Cisco Press, pp: 206.
10. Ostapenko, A.G., 2009. Prospects of the Development of the System Risk Analysis Methodology / Ostapenko A.G., Karpeyev D.O., Plotnikov D.G. // Information and Security, 3: 419-424.
11. Ostapenko, A.G., 2013. The Risks of Disbenefit, Chances of Benefit and Robustness of Automated System Components When Faced the Impact of Information Threats / Ostapenko A.G., Yermilov Y.V., Kalashnikov A.O. // Information and Security, 2: 215-218.