DEFENCE AGAINST DDOS

Kamil DUŠEK, Doctoral Degree Programme
Department of Telecommunications Engineering, FEE,
Czech Technical University in Prague, Czech Republic

E-mail: dusekk@fel.cvut.cz

ABSTRACT

Security has been an important issue in the Internet for several years. Besides the security of data communication there is a problem with the security of the network itself. Denials of Service (DDoS) attacks [1] are considered among the latter. A special form of DoS is Distributed DoS. In this case the attack is launched from hundreds or thousands of machines towards a victim. A principal concept of a DDoS network of an attacker is depicted on the Figure 1. The main purpose of the following text is to describe defense against DDoS attacks with suggestions for future work.

1 DEFENCE AGAINST DDOS

The principal DDoS network is depicted on the Figure 1. Attacker uses a Client to command hundreds or thousands Agents through several Handlers. Agents generate attacking packets towards the Victim.

There are two steps building up such a DDoS network. Firstly, several machines are compromised exploiting some flaws in software (usually servers running on the machines). The Handlers and Agents are deployed and set up in the second step.
The simple defense against the first step is to keep up with the latest software releases and patches. Recent DDoS attacks prove that this is hard to realize in practice. There is likely to continue in future. Thus there will be always backdoors settled within Internet. There are commercial and free solutions that can test vulnerability of the machines on the Internet, for example Nessus [2].

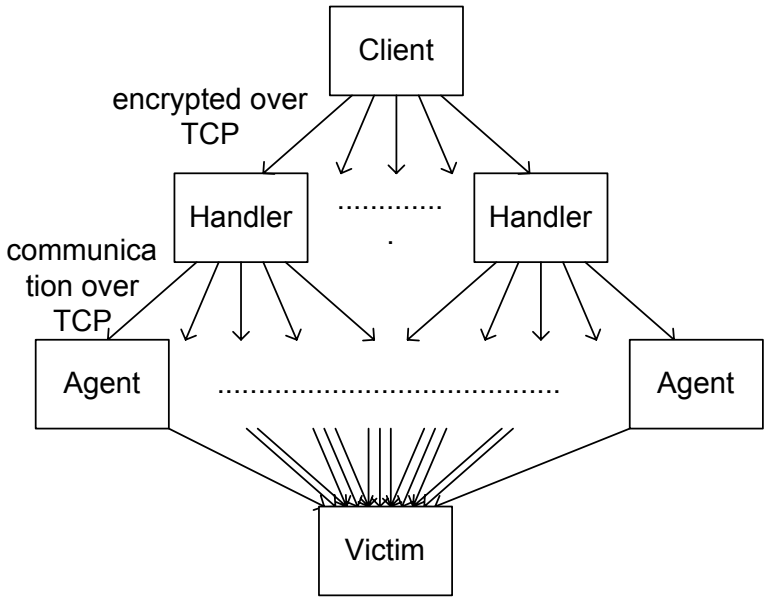

Fig. 1: *Typical DDoS network.*

Once the DDoS network has been set up there are three points in the defense: detection and suspension of attack, and tracking down of the initiator of the attack (Client on the figure). There is number of different DDoS attacks but they have something in common. They spoof the source address in the attacking IP packets. The attacker checks out whether the network of each Agent permits address spoofing while building the DDoS network. Spoofed packets could be filtered out in the networks. This could be probably thought of as the best protection against DDoS attacks. Again this is hard to accomplish in the real Internet in near future.

Otherwise the attacking packets are hard to distinguish in the traffic. Hence the anomalies in the statistical characteristics of the traffic are used to detect DDoS attack. This is the case of HIDE [3] or Traffic Master Inspector [4].

Suspension of the DDoS means filtering out the attack packets. The closer to the Agents the filtering takes place the more effective it is.

The initiator of the attack is on the top of the DDoS tree and the attack can be scheduled beforehand. Moreover there is a trend to use encrypted communication among entities of a DDoS network. Thus the initiator could be tracked usually after the attack supposing that the nodes keep such a database where communication between Client and Handlers can be found.

2 CONCLUSIONS

The control of IP source address in the worldwide scale of the Internet is not feasible in near future. The flow of the attacking packets goes through several nodes on the way to the Victim. The detection and suspension of an attack is most effective on the opposite sides of the Agent-Victim path. While the attack can be detected easily at the point of the Victim the filtering of the attacking packets is effective on the other hand close to the Agents. It seems that a distributed defense network could be able to detect and protect effectively against DDoS attacks.

HIDE [3] or Traffic Master Inspector [4] use statistical anomalies to detect DDoS attack

while monitoring all traffic. Probes monitoring traffic at high-speed networks use packet sampling to ease performance needs. Such probes could be used as the members of the distributed defense network. The attack detection while using the method of packet sampling shall be investigated.

Once DDoS attack has been detected it should be suppressed as close to the Agents as possible in order not to load the network with attacking packets. An integration of the distributed defense network and common network infrastructure shall be investigated as well.

REFERENCES

[1] R. K. C. Chang, Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial, Communications Magazine, Oct. 2002

[2] Nessus, http://www.nessus.org.

[3] C. Manikopoulos, S. Papavassiliou, Network Intrusion and Fault Detection: A Statistical Anomaly Approach, Communications Magazine, Oct. 2002.

[4] Mazu networks - Inspector, http://www.mazunetworks.com/products/profiler.html