Denial of Service on TCP/IP Security Protocols: Vulnerabilities, Tools and Countermeasures

Kamini Nalavade\textsuperscript{1}, B.B. Meshram\textsuperscript{2}

\textsuperscript{1}Research Scholar, Computer Engineering Department, V.J.T.I.,
Matunga, Mumbai
kamini.nalavade@live.com
\textsuperscript{2}Professor & Head, Computer Engineering Department, V.J.T.I.,
Matunga, Mumbai
bbmeshram@vjti.org.in

ABSTRACT
TCP/IP protocol suite, the adapted standard for communication over network, suffers from inherent vulnerabilities in the design of underlying protocols. These vulnerabilities are the main source of various attacks. Security protocols are included in the original TCP/IP suite to provide integrity, availability and confidentiality to the data moving on networks. But these security protocols are also vulnerable to different attacks such as DOS, Sniffing etc.. Denial of Service attack is an attack which makes an online information or network resource unavailable to legitimate users. This paper attempts a comprehensive study of vulnerabilities and the Denial of Service problem in security protocols such as IPSec, SSL, and PGP of TCP/IP suite. The major contribution of this paper is that it helps to classify the different techniques used in a DoS attack, and discuss tools used in setting up a DoS attack over network. We propose architecture for Intrusion Prevention Systems for protecting information processed in Security protocols.

Indexing terms/Keywords
Network; Attacks; Vulnerabilities; Protocols and Defense

Academic Discipline And Sub-Disciplines
Engineering, Network Security

SUBJECT CLASSIFICATION
Intrusion Detection and Prevention

TYPE (METHOD/APPROACH)
Vulnerability and Attack Classification
INTRODUCTION

The continuous improvements in new technology have enabled the use of computer systems for gathering and sharing information using the Internet. The information flow on Internet is constantly under various attacks because of vulnerabilities lying in the structure of communication networks. The adapted standard for communication over network is TCP/IP which has many flaws in it. These vulnerabilities are the main source of attack. Adapting totally new architecture for Internet for all users is difficult to implement. Due to a number of attacks reported on private networks originating from the Internet, security has become a primary concern for corporations using the Internet.

To overcome these flaws in present TCP/IP architecture addition of security protocols is done at each and every level. These protocols were successful in providing security to some of the important aspects of network but these protocols themselves suffer from vulnerabilities. Some of these vulnerabilities are the new source to potential denial of service attacks. Because of this reason study of security protocols, their architecture and related vulnerabilities is very important.

Denial of Service (DOS) attack is an attempt to make an online network resource unavailable to its legitimate users. A resource can be anything from a personal computer, router, network infrastructure, web services or any other possible entity on the network, intra-net or internet. The DoS attacks have manifested its dangerous impact frequently on the internet architectures. The DoS attacks are becoming common and easy to execute day after day. The attackers are building more sophisticated tools and strategies to produce the DoS attacks. Today, anyone with an adequate computer skills and decent internet connectivity can launch DoS attack with a click of mouse.

Certainly, this is one of the biggest threats to any business that is dependent on availability of its services on the internet. These attacks can be classified into two broad categories. The first category is a simple case where an attacker launches the attack from single computer. The other category includes the DoS attacks that involve the participation of more than one computer to execute the DoS attacks. As this attack is conducted from different locations, it is called as DDOS or Distributed Denial of Service attack. The distributed machines could consist of compromised computers which are known as zombies, or machines belonging to multiple people who are perpetrating the attack as a result of concerted efforts. The effect of DDOS attack is likely to be more destructive as compared with the simple DOS attack described earlier. In this paper we explain vulnerabilities and defense against Denial of Service attack for some of the important security protocols.

In next section we describe vulnerabilities and Dos attack on IPsec protocol with defense techniques. Section III and IV describes vulnerabilities causing DOS in SSL and DNSSec protocols respectively. Section V provides our Intrusion Protection Model. Section VI summarizes the study followed by conclusion.

IPSEC: VULNERABILITIES, ATTACK AND DEFENSE

IPsec is a suite of protocols for securing network layer. The major flaw in IP protocol is that it does not provide authentication. IPsec protects the intrusions on Internet Protocol (IP) communications by providing authentication. IPsec encrypts each IP packet of a data stream. IPsec includes two major protocols: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH protects message integrity and authentication. Also it provides replay protection. ESP provides confidentiality of the exchanged data. Both protocols are located in the network layer to protect messages. IPsec can be used to protect data flows between a pair of hosts e.g. computer users or servers, between a pair of security gateways e.g. routers or firewalls, or between a security gateway and a host [5]. A critical aspect of IPsec, is automatic key management, keying material and security suite requirements. Internet Key Exchange is the automatic key management protocol used for IPsec. IKE was created from several other key management protocols and is the default for IPsec, but other key management protocols can also be used. In reality, no key management is required for IPsec functions and the keys can be manually managed. However, manual key management is not desirable for all implementations due to the administrative overhead and the fact that keys never expire. Having keys that never expire represents security vulnerability.

When packets flow across a network, an attacker might predict sensitive information by viewing source and destination addresses provided in the IP header. For example, Alice is exchanging high-volume traffic with Bob; an attacker might use addresses to reconnaissance topology of network, causing denial of service (DOS) attacks. In this kind of attack a hacker floods server with requests that block access to legitimate users. To keep addresses private, IPsec can be used in tunnel mode. The entire private IP packet, header and payload are hidden inside a public IP packet. A number of articles on the bugtraq mailing list, Dec 2001 discussed the discovery of a Denial of Service (DOS) attack that could be launched on Windows 2000 machines that use IPSEC. The discovery showed that sending UDP traffic to port 500 of a Windows 2000 machine could raise the processor usage up to 99% on a high-end machine and render it incapable of communication. The advisory suggested that fire walling port 500 off would be an effective solution. The listings also noted that most VPN configurations implement a packet filter that only accepts connections on port 500 from known clients and would not be susceptible to this attack.

The IKE protocol is used in the Internet Protocol Security (IPsec) protocol suite to negotiate cryptographic attributes that will be used to encrypt or authenticate the communication session. These attributes include cryptographic algorithm, mode, and shared keys. The end result of IKE is a shared session secret that will be used to derive cryptographic keys.
SSL: VULNERABILITIES, ATTACK AND DEFENSE

Secure Socket Layer Security protocols provide a secure channel between two machines over the intranet/internet. It facilitates the authentication of the communicating parties to each other and confidentiality and integrity of the communication between them. Any protocol that can be run over transport layer protocol such as the TCP (Transmission Control protocol) can be run over the SSL with minimal modification. The SSL protocol involves the number of cryptographic operations. The public key cryptography is used to perform authentication and key exchange process. The key negotiated through the key exchange process is processed to generate the symmetric key that is used to protect the communication between the server and the client. The general procedure of encrypted communication is the following:

1. The client and the server select a encryption algorithm for encrypting the communication.
2. The client authenticates the server by requesting its certificate. Optionally, the server can also request a certificate from the client, thus mutual authentication is also possible.
3. The client encrypts his message using symmetric a key.
4. The client transmits the message to the receiver.
5. The server decrypts the message using a symmetric key.
6. The communication between the parties can continue by repeating steps 3-5. The server stores information including the session ID and other parameters about past SSL/TLS session in its session cache. Clients that have contacted a particular server previously can request to continue a session by identifying its session ID. This can be used to accelerate the initialization of the connection.

Unfortunately, process of key exchange and authentication, especially when the RSA method is used, are the most expensive operations on the server to perform. The client, however, can get away with this operation with a little investment of the memory and computational resources. Therefore, clients can easily open a number of new SSL connections to request a server to perform such computationally expensive operations without doing any significant work themselves. This leads to the fact that an attacker can deploy DOS attacks by generating too many requests probably from multiple sources to exhaust the computational resource of the target server.

The SSL protocol has one feature called SSL Renegotiation. This feature is easily exploitable to execute the computational DoS attack on the SSL web servers. The SSL renegotiation is the process of starting a new handshake in an existing SSL session. The handshake conducted during the renegotiation is protected under existing session state. The normal SSL handshake is conducted in the plain text. The renegotiation handshake protocol messages are encrypted unless the existing session uses NULL cipher. This is the only difference between the usual handshake and the handshake carried out during the SSL renegotiation. Intuitively, the SSL renegotiation handshake is as expensive as usual SSL handshake. In traditional DoS attack, the attacker opens a numerous SSL connections with the server to computationally exhaust the server. However, with the help of renegotiation features in the SSL protocol, the attacker does not have to open many connections to increase the computational overhead on the server. The attacker can simply open a single connection and renegotiate multiple times under the same SSL connection.

The SSL handshake is the culprit behind the computational overhead. At the end, motivation behind the attack is to computationally exhaust the SSL server. The simplest way to mitigate renegotiation based DoS attack is to disable the renegotiation feature on the server side.

The administrator of the server should consider the requirement of his server and take appropriate action about disabling the SSL renegotiation. SSL renegotiation can be initiated both by the clients as well as the servers. The better choice would be to disable the client initiated renegotiation.
One of the important reasons for the SSL to be the target of the DoS attacks is the unbalanced work overhead. The server is the one who has to perform the RSA decryption operation as opposed to the client who performs the comparatively cheaper operation such as RSA encryption. The other operations involved in the SSL protocol are same on the both connection ends and therefore, do not contribute to the uneven distribution of the work overhead. These operations include the MAC calculation, master secret generation, etc. Once, the SSL handshake is completed, the symmetric key operations are very much cheaper than the public-key operations performed during handshake and these operations need to be performed on the both sides. The tools which can be used for DOS attack are sslsqueeze tool, thc-ssl-dos tool and BFC tool.

DNSSEC: VULNERABILITIES ATTACK AND DEFENSE

The Domain Name System (DNS) is a distributed database that stores host names and their corresponding Internet Protocol (IP) addresses in the servers. It provides service of translating the domain names from its human readable form to machine readable IP addresses and vice versa. Since the information stored in the DNS servers is sensitive, it is essential to provide security to it. The DNS was not designed with security in mind and is prone to various attacks. Due to the lack of a security layer over the DNS system, the DNS queries can be manipulated and the user can be redirected to a malicious website. An attacker can use DNS spoofing to modify the server responses and send it back to the legitimate users.

DNS is prone to Denial of Service attacks as in the case of network service. The application of security techniques to overcome this threat seems to make it worse as it adds overhead for every DNS message and can add to the number of messages being sent. DNS Amplification effect in a recursive DNS attack is based on the fact that small queries can generate larger UDP packets in response. An attacker can spoof a query and cause the reply from the DNS servers to be delivered to another host. The attack can be distributed among several recursive and authoritative name servers in order to be more difficult to block. Although the victim can use a security policy that distinguishes and ignores the unwanted DNS traffic, still if the traffic is more than the available bandwidth before the point where it is blocked, a bottleneck can be created. DNSSEC’s responses are more suitable for the attack, because of the embedded public keys and signatures in the DNSSEC resource records. The larger response size allows DNSSEC to have higher amplification ratio for this attack compared to DNS. RFC5358 [13] suggests limiting the DNS DoS amplification attacks by denying traffic from spoofed source IP addresses. Possible solution is implementing ingress filtering a technique for checking if packets originate from the networks they claim to be from.

Zone transfers are performed to replicate zone files in multiple servers to provide a degree of fault tolerance in the DNS service provided by an organization. As zone transfers involve the transfer of entire zones, they overload network resources relative to normal DNS queries. Malicious zone transfer requests on the name servers can overload the master zone server and result in denial of service. The denial-of-service can be minimized if servers are allowed to make zone transfer requests to a set of known entities. Name server software such as BIND initially provided a configuration feature to restrict zone transfer requests to a set of predefined IP addresses. But as IP addresses can be spoofed, antispoof protection is required as an additional feature. The tools DNSSEC Walker and Nessus were found useful for performing penetration tests on DNSSEC enabled name servers.

PROPOSED SYSTEM ARCHITECTURE

Denial of service is the prime concern for any organization having its resources on-line. The security protocols are also victim of DOS attacks. Here we propose Intrusion Prevention architecture to be placed in a router to provide security from DOS attack.
Our proposed system architecture is shown in figure above. The packet capture and filtering provides filtered output from input packet stream. This decomposition will help to provide detection of protocol related intrusions faster and efficient way. DNSsec detection is to detect the size of the DNS reply is crossing 4000 bytes or not. And to monitor DNS queries going to the DNS Server. SSL attack detection check the renegotiation request in a ongoing session by keeping track of session IDs. IPSec intrusion detection provides monitoring of UDP packets and it port numbers. This will stop flooding of UDP packets to the port 500 to the servers.

The system provides packet filtering, Content filtering and Session monitoring features. Also the configuration settings can be modified using the features provided in the system. We have considered three protocols for the DOS intrusion SSL, IPSec and DNSSec. We are considering IPSec UDP flooding attacks, SSL renegotiation attacks and DNSSec amplification attacks. The Dos attacks on these three protocols are already discussed in the previous sections. The detection methodology works as follows:

1. IPSec UDP flooding: For detecting attacks, UDP traffic is monitored and packets with port no 500 are inspected. Counter is set for every known and friendly entity. If the sender is from known entities and counter is below threshold then packet is allowed. Otherwise packet will be discarded.

2. SSL renegotiation attacks: SSL renegotiation can be initiated both by the clients as well as the servers. The better choice would be to disable the client initiated renegotiation.

3. DNSSec Amplification Attacks: Source address verification at routers for DNS Queries and also drop reply from DNS servers having more than 4000 bytes.

As far as Denial of Service attacks is considered no one can stop but can be avoided and stopped before they completely affect systems on the server. Our approach is simple and novel, without any modification to the existing system. Some extra functionality can be added to the router to avoid above stated attacks.

RESULTS AND DISCUSSION

System implementation is done with router simulator GNS3 and Java programming. The Router was programmed to receive packets generated through packet crafting tools. The captured packets are filtered as IPSec, SSL or DNSSec packets. Separate log files were created for the protocols. We tried our system on the packets stream of 10000 packets consisting of 350 Ipsec packets, 210 SSL packets and 240 DNSsec queries. The other packets were of traditional TCP/IP protocols. 10% from every stream were compromised intentionally to carry intrusions. Our system runs on the above data. Two parameters were considered for the results, false alarms generated and time for intrusion detection. The false alarms generation rate was 65% for IPSec, 57% for SSL and 49% for DNSSec in first run. The results were improved when the training data size was increased by 50%

RESULTS AND DISCUSSION

System implementation is done with router simulator GNS3 and Java programming. The Router was programmed to receive packets generated through packet crafting tools. The captured packets are filtered as IPSec, SSL or DNSSec packets. Separate log files were created for the protocols. We tried our system on the packets stream of 10000 packets consisting of 350 Ipsec packets, 210 SSL packets and 240 DNSsec queries. The other packets were of traditional TCP/IP protocols. 10% from every stream were compromised intentionally to carry intrusions. Our system runs on the above data. Two parameters were considered for the results, false alarms generated and time for intrusion detection. The false alarms generation rate was 65% for IPSec, 57% for SSL and 49% for DNSSec in first run. The results were improved when the training data size was increased by 50% and false intrusions were also increased. The system results proved that packet filtering and session monitoring at routers can improve the intrusion detection. Although it is time consuming to inspect packets at the router one by one. But we can improve our approach by applying the inspection at session level. This will help to keep an eye on suspected hosts and prevent denial of service as early as possible.

SUMMARY

Here we summarize the study of vulnerabilities, tools and attacks on IPsec, SSL and DNSSec protocols.

<table>
<thead>
<tr>
<th>Protocol and Vulnerability</th>
<th>Tools</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec- 1. “encryption-only” ESP configuration. 2. sending UDP traffic to port 500 of a Windows 2000 machine could raise the processor usage up to 98% on a high-end machine and render it incapable of communication.</td>
<td>Sslsqueeze thc-ssl-dos tool BFC tool</td>
<td>1. Fire walling port 500 off would be an effective solution. 2. Cisco has released free software updates that address the CISCO IOS vulnerability causing DOS.</td>
</tr>
<tr>
<td>SSL- 1. the unbalanced work overhead 2. clients can easily open a number of new SSL connections to request a server to perform computationally expensive operations. 3. SSL Renegotiation. This feature is easily exploitable to execute the computational DoS attack on the SSL web servers.</td>
<td></td>
<td>1. The symmetric key operations performed during handshake need to be performed on the both sides. 2. The administrator of the server should consider the requirement of his/her server and take appropriate action about disabling the SSL renegotiation. 3. Statefull Firewalling</td>
</tr>
<tr>
<td>DNSSec</td>
<td>DNSSEC Walker Nessus</td>
<td>Denying traffic from spoofed source IP addresses. Possible solution is implementing ingress filtering. Recursive lookup on authoritative servers to be disabled by name server administrators. Clients can use internally available recursive name servers. In this way an attacker will not be able to abuse the recursive name servers for DNSpilification attack.</td>
</tr>
</tbody>
</table>
TCP/IP protocol suite, de facto standard for communication over Internet have many inherent design flaws. It is impossible to completely change the networking base for communication. So to protect information flow from attackers various security protocols are added to the basic TCP/IP protocol suite at every layer such as IPSec at network layer, SSL/TLS at transport layer, and DNSSEC at application layer. The purpose of these protocols was providing security but as the time passed, new vulnerabilities were discovered in the protocol design. These vulnerabilities caused many serious attacks such as DOS. Here we described the vulnerabilities and how Denial of Service takes place because of these vulnerabilities. The different tools and defense for the attack is also explained in detail.

REFERENCES


Vesselin Hadjitodorov, “Security of IPv6 and DNSSEC for penetration testers”, Research Project University of Amsterdam, July 2011


http://www.ccs.neu.edu/home/guttman/ransm.pdf


Author' biography with Photo

Kamini C. Nalavade received the B.E. degree in computer science and engineering from the SGGGS, College of engineering and technology, Nanded in 2001 and M.Tech degree in computer engineering from Veermata Jijabai Technological Institute (VJTI), Mumbai in 2007. She is currently PhD student in the department of computer engineering, VJTI, Mumbai. Her research interest includes intrusion detection, network security, data mining and data privacy.

Dr. B. B. Meshram is currently professor and Head of Computer Technology Department of Veermata Jijabai Technological Institute (VJTI), Matunga, Mumbai (INDIA). His areas of interest include Object oriented database management systems, Computer network security and multimedia systems. He has published more than 200 papers in National & International Conferences & refereed Journals.