ABC SBC: VoIP Border Control

FRAFOS GmbH

Introduction

One of the most widely observed fraud scenarios is the case of a malicious user detecting the address of a PSTN gateway and accessing that gateway directly. Once the attacker has managed to access the gateway the attacker can start selling telephony minutes through that gateway.

The ABC SBC establishes a secure border between the VoIP service provider's core VoIP components–e.g., PSTN gateway, SIP proxy and application servers- and the subscribers. As the border element, the ABC SBC hides the details of the operator's network from subscribers and absorbs any attacks and sudden spikes in the subscriber traffic. Further, the mediation features of the ABC SBC shield the operator's network from malfunctioning user agents and any interoperability issues.

Topology Hiding

As the result of a SIP session establishment the involved end points will have exchanged the IP addresses of where to send and receive media traffic. This means that a user using VoIP for calling a PSTN number will know the IP address of the PSTN gateway that is responsible for bridging the VoIP service with PSTN. Further, during the session establishment all the involved proxies will include their addresses in the Via headers.

A malicious user could use this information to either attack an operator's proxy or even get access to the PSTN gateways directly. By having the ability to contact the PSTN gateways directly, an attacker can misuse any security holes that might exist at the PSTN gateway. This would allow the attacker to initiate calls to the PSTN with the costs being incurred on the service provider.

When deploying the ABC SBC as the interconnection element to other operators, the ABC SBC hides all information about the internal components of the operator before forwarding them to a neighbor. The ABC SBC replaces the addresses of internal components with its own. Hence, headers such as contact, Via, Record-Route, Route and so on would include the ABC SBCs address only.

Depending on the level of trust established with a certain neighbor, the ABC SBC can be configured to also route the media traffic and hide the internal addressing information of the media handling components.

Denial of Service and Overload Protection

If we have learned one thing from the Internet, then it is that there will always be some people with enough technical skill and time to figure out a way to attack some service. The ABC SBC protects the operator's VoIP service from DoS attacks or a sudden increase in the number of calls, e.g., Christmas calls.

In order to keep the malicious traffic and overload away from the core servers, e.g. applications servers, proxies and PSTN gateways, the ABC SBC supports the following protection mechanisms:

- **Traffic limitation:** Service providers can limit the rate of incoming calls and registrations. Once these limits are exceeded, the ABC SBC starts rejecting messages arriving in excess of these limits. These limits can apply to single sources, e.g., accept no more than X REGISTER requests from source Y, or a range of senders or to all incoming traffic.
- **Content filtering:** An attacker could try to get access to some protected resources by launching an SQL injection attack or try to bring a server down by sending SIP messages with malformatted content. By analyzing the content of incoming SIP messages and rejecting messages that seem to include malicious content, the ABC SBCs can protect the core components of the network.

NAT-Traversal Support

Network Address Translators (NAT) are used to overcome the lack of IPv4 address availability by hiding an enterprise or even an operator's network behind one or few IP addresses. The devices behind the NAT use private IP addresses that are not routable in the public Internet.

In case a user agent is located behind a NAT then it will use a private IP address as its contact address in the Contact and Via headers as well as the SDP part. This information would then be useless for anyone trying to contact this user agent from the public Internet.

The ABC SBC acts as the public interface of the user agents behind a NAT and routes both signaling and media traffic to the user agents.

Access Control and Fraud Prevention

The ABC SBCs controls which users and what messages can cross the borders of a VoIP infrastructure and use the offered VoIP services. This is achieved by a number of features:

- Media access control: The ABC SBC allows media traffic from a subscriber only after the successful signaling of a call. Further, The ABC SBC blocks traffic with unwanted codecs and limits the amount of traffic that can be sent by a subscriber.
- Fraud prevention: Prices for a flat rate service are determined based on a certain expected user behavior. However, operators often face the case that a user subscribes for a flat rate telephony residential service but then starts reselling telephony minutes. This kind of behavior causes substantial financial losses to the service provider and overloads the network. To suppress this fraud possibility, the ABC SBC limits the number of parallel calls generated by a user as well as the duration and frequency of calls.

Registration Offloading

In order to reduce the number of registrations that have to be processed at the operator's registrar, the ABC SBC will cache successful registrations. The registration information at the operator's registrar will be refreshed by the ABC SBC at much lower rates than the subscribers refresh attempts. This will reduce the load on the operator's infrastructure and will protect it from misbehaving subscribers or malicious users that try to attack the network by sending large numbers of registration messages.

Interoperability Mediation

With different standardization groups working on SIP and the different interpretation of developers to the same specifications, interoperability between SIP components of different manufacturers and for different network architectures is unfortunately not always guaranteed.

The ABC SBC offers a powerful GUI based mediation functionality that enables an operator to adapt incoming and outgoing traffic. Using the ABC SBC mediation GUI, a service provider can configure the following actions:

- Stateless SIP header manipulation: The ABC SBC can be configured to remove certain headers and add others.

- Statefull message handling: To support the differences between the IMS and IETF specifications the ABC SBC is capable of overcoming differences in the call flows and generating appropriate responses and requests.
- Message blocking: The ABC SBC drops/rejects requests and messages not supported by an operator.
- Header manipulation: The ABC SBC can be configured to change the content of a certain header.
- Transport mediation: SIP can be transported over UDP, TCP and SCTP. Further, it can work over IPv4 and IPv6. The ABC SBC can enable two elements using different transport protocols to communicate seamlessly with each other.
- Media transcoding: The ABC SBC supports software based transcoding of media.

System and Network Monitoring

Through the management GUI the operator of the ABC SBC can have an elaborate overview of the performance of the VoIP infrastructure and be alerted to failures. The monitoring interface of the ABC SBC provides the following information:

- General statistics (memory, CPU and bandwidth usage)
- SIP statistics (number of sessions, packets)
- Call flow diagrams visualization
- Collection of call traces in PCAP format

Capacity

The ABC SBC supports up to 7000 simultaneous calls running with G.711 codec on the standard hardware offered by FRAFOS. To scale an interconnection point more nodes with each node getting its own IP address can be added. In case an entire interconnection point is to be reached by a single address then FRAFOS also offers a SIP-load balancing solution that enables the operator to cluster a number of ABC SBCs behind a single entry point.

Announcement and Recording

The ABC SBC offers an extensive range of media handling capabilities and interfaces offering applications such as announcements, recording and music on hold. Service providers can use these capabilities to offload part of the application logic and processing from their application servers. For example, calls that are destined to subscribers not served by the operators can be rejected using an announcement indicating: “Destination is unknown”. This is usually achieved by routing a call to an application server that would generate this announcement. With the ABC SBC the call flow optimized by generating the announcement directly at the border of the network.

Technical Specifications

SUPPORTED PLATFORMS

Linux

SIGNALING FEATURES

SIP RFC compliant

B2BUA

SIP header manipulation

Multi-part body support

Registration offloading

MEDIA SERVICES

Software based transcoding (G711u/a, G726, GSM, iLBC, L16,G722, Speex; on request: G729a, G729a/b, AMR)

Dynamic jitter control

NAT/NAPT on media

Audio codec relay

Video codec relay

RTP inactivity monitoring

Codec filtering

MANAGEMENT CAPABILITIES

GUI based configuration and monitoring

Secure embedded web-based GUI

SSH access

SNMP V2 status and logs

Local logging of alarms, events and statistics

CALL ROUTING

Call blocking and filtering

Embedded routing engine

QOS CONTROL

Bandwidth limitation and management

Call admission control per peering partner/trunk

PROTOCOL SUPPORT

SIP

RTP

UDP, TCP, SCTP

Translation between transport protocols

SNMP, NTP, SSH, DNS

SECURITY

Signaling topology hiding

Media topology hiding

RTP DoS protection

Call rate limitation

Parallel call limitation

HIGH AVAILABILITY

Active/Hot Standby redundancy model

REFERENCE HARDWARE

CPU: 2x HexaCore with HyperThreading

RAM: 48GB

HDD: RAID-10 with 4 disks, 15K RPM

Network interfaces:

- Management ports
  - Two (active/standby) 10/100/1000 Ethernet RJ-45 ports
- Media/signaling High availability Ports
  - Four 1 Gbps Ethernet RJ-45

About FRAFOS

FRAFOS GmbH is a manufacturer of VoIP solutions with offices in Berlin and Prague. FRAFOS was incorporated as privately held company in May 2010, in Berlin, Germany.

The history of FRAFOS team and technology goes back to the late nineties. As researchers at the prestigious German public R&D institute Fraunhofer FOKUS, the FRAFOS founders were the among the first to work the SIP and RTP standards and to develop open source solutions that paved the way for the VoIP revolution.