ABC SBC: Securing the Enterprise

FRAFOS GmbH

Bismarckstr 10-12

CHIC offices

10625 Berlin

Germany

www.frafos.com

Introduction

A widely reported fraud scenarios is the case of a malicious user detecting the address of a company's PBX and accessing that PBX directly. Once the attacker has managed to have access to the PBX the attacker can start making calls and even sell telephony minutes through that PBX with the costs incurred upon the owner of the PBX.

The ABC SBC establishes a secure border between the enterprise VoIP solution and the rest of the world. As the border element, the ABC SBC hides the details of the enterprise solution and absorbs any attacks and fraud attempts. Further, the mediation features of the ABC SBC shield the enterprise 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 the enterprise will know the IP address of the enterprise PBX.

A malicious user could use this information to try and get access to the enterprise PBX. By having the ability to contact the PBX directly, an attacker might be able to misuse any security holes that might exist at the PBX. This would allow the attacker to initiate calls through the PBX with the costs being incurred on the enterprise.

When deploying the ABC SBC as the interconnection element between the enterprise and the VoIP service provider, which are serving the enterprise, the ABC SBC hides all information about the PBX before forwarding them to the VoIP service provider. The ABC SBC replaces the address of the PBX with its own. Hence, headers such as Contact, Via, Record-Route, Route and so on include the SBCs address only.

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 an enterprise 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 PBX the ABC SBC supports the following protection mechanisms:

- **Traffic limitation:** An enterprise can limit the rate of incoming and outgoing calls. Once these limits are exceeded, the ABC SBC starts rejecting calls arriving in excess of these limits. These limits can apply to either the entire enterprise or to single sources, e.g., number of calls from some department should not exceed some limit, or to certain destinations, e.g., no more than X long distance calls can be conducted in parallel.
- **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 enterprise PBX and VoIP solution.

NAT-Traversal Support

Network Address Translators (NAT) are used to overcome the lack of IPv4 address availability by hiding an enterprise 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 there is a NAT between the PBX and the SBC then the ABC SBC can offer NAT traversal support. In general one could, however, expect the PBX and the enterprise SBC to be in the same network. In this case the ABC SBC acts as a NAT. This is achieved by having two interfaces at the ABC SBC with one of them private and the other public with the PBX connected to the ABC SBC over the private one. The ABC SBC uses its public address to communicate with the VoIP service providers. Unlike NATs which only mangle the IP addresses in the IP headers, the ABC SBC includes its public IP address in the contact, routing and body parts of the SIP message.

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:

- **Access control:** In order to protect the PBX, the ABC SBC only accepts calls arriving over a secure connection established with a trusted VoIP operator. The trust relation can be established using TLS or IPSEC.
- **Fraud prevention:** By using blacklists the administrator of the enterprise's VoIP service can limit the destinations to which the enterprise users can call. This helps in protecting against the case that an attacker manages to get access to the PBX and starts calling expensive service numbers or exotic countries.

Interoperability Mediation

With different standardization groups working in SIP and the different interpretation of developers to the same specifications, interoperability between SIP components of different manufacturers and of different network architectures in 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, an operator 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 AB 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 enterprise.

- 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.

Capacity

The ABC SBC supports up to 5000 simultaneous calls running with G.711 codec on off the shelve hardware. For smaller enterprises, FRAFOS also offers the ABC SBC as a software only solution that can be deployed on top of hardware chosen by the enterprise. The ABC SBC can also be integrated into a virtualized environment on top of already available hardware. The capacity of the ABC SBC will depend then on the used hardware and available resources.

Technical Specifications

Supported Platforms Linux	**High Availability** Active/Hot Standby redundancy model
WebRTC Features Javascript SIP over WebSocket NAT traversal using ICE, TURN, STUN JsSIP support	**QoS Control** Bandwidth limitation and management Call admission control per peering partner/trunk
Media Services Routing audio codec including G.711, OPUS. Routing of video codec including VP8 Dynamic jitter control NAT/NAPT on media RTP inactivity monitoring Codec filtering	**Call Routing** Call blocking and filtering Embedded routing engine Load balancing Peer monitoring and availability detection Alternative routing on failure Table based routing for LCA
Media Applications Call recording Announcement services Software based transcoding (G711u/a, G726, OPUS, iLBC, L16, G722, Speex; on request: G729a, G729a/b, AMR)	**SIP** Registration pass-through Registration caching and offload SIP header manipulation SIP Back2Back UA
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 REST and XML RPC based open interfaces	**Protocol Support** UDP, TCP WebSocket Translation between transport protocols Per source/destination transport layer mediation SNMP, NTP, SSHDNS RTP, RTCP, SRTP TLS, DTLS, SDES
Virtualization	**Hardware**

Amazon cloud Virtualization software OVM, KVM ..	Hardware independent

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.

FRAFOS offers SIP session management and security solutions of the latest generation that come either as a standalone solution or as a cloud ready implementation. The flagship product of FRAFOS, the ABC SBC, offers open interfaces and built in multimedia applications such as recording and announcements. The ABC SBC enables the service providers and enterprises to simplify their service infrastructure and prepares them for future challenges.