SBC: Do I really need it?

Prepared by: Md. Abul Bashar Azad
abazad@office.bdcom.com
Bangladesh Safe home for foreign VOIP frauds
RAB arrested 37 Chinese and Taiwanese nationals and seize  
(Dhaka tribune 2014 )

BTRC asks telcos to check call spoofing (prothomalo 2016)

BTRC alerts mobile users to frauds  
(https://www.thedailystar.net 2016)

FBI finds Philippine hackers Compromised AT&T network and used their phone systems to call others long distance phone number. AT&T losses of up to $2.0 million (November 2011)

Massive DDoS attacks a growing threat to a VoIP service.  
It crashes TelePacific VoIP system.  Average 34 million SIP traffic VoIP connections requests in 1 day and flooding their systems (March 2011)

The global telecom industry annual losses of $46.3 Billion due to toll fraud  
According to the Global Loss Survey 2013 of the communications Fraud Control Association (CFCA)
Abuse Methods in telecom industry

Top 5 Emerging Fraud Methods

- Identity Theft: 6.00%
- Dealer Fraud: 7.00%
- VoIP Hacking: 10.00%
- Subscription Fraud: 10.00%
- PBX Hacking: 12.00%

Communications Fraud Control Association survey report
What is sip?

- **Session Initiation Protocol (SIP)**
  - SIP (Session Initiation Protocol) is a protocol used in VoIP communications allowing users to make voice and video calls over the internet.
  - Types of devices use - computers, phone set, IP-PABX, video equipment, media gateway, soft switch etc. - can exchange data over SIP
SIP Threat Categories of IP-Telephony service provider Networks

- Fuzzing Attacks
- VOIP Network Eavesdropping
- VOIP network Interception and Modification
- Device Configuration Weakness
- Voice & Telephony Denial of Service (TDOS) Attacks
- Device and OS Vulnerabilities
- IP/TCP Network Infrastructure Weakness
- VOIP & UC Protocols Implementation Vulnerabilities
- RoboCalls
- SIP BotNet attacks
- Signaling Manipulation Attacks
- Fraud Attacks – Wangiri, IRSF and many others
- Media Manipulation Attacks
- SPAM over Internet Telephony (SPIT)
- UC Infrastructure Threats (Voice, Media, IM, Web, UC & Collaboration)
- UC Application Layer Threats
- Data and Voice Threats
- Voice Phishing
Phase of a VOIP/SIP Attack

1. **SIPVicious**
   - Discovery, Password Cracking
   - Denial of Service Flooding
   - Memory Corruption

2. **SIPp**
   - SIPsak
   - SipNESS
   - Invite Flooder
   - RTP Flooder

3. **Fuzzer**

4. **Soft Switch**
   - Use SIP

5. **Extension Hijacked**
   - Full Excess Control
IP-Telephony core system security hole

IP Telephony Core System Diagram
What is SBC?

A Session Border Controller (SBC) is a dedicated hardware device or application that governing calls on a VOIP network. It’s allowing only authorized session pass through the connecting point.
How to Deploy SBC?

SBC Deployment Diagram

- Internet Cloud
- SBC
- Soft Switch
- Media Gateway
- ICX - 1
- ICX - 2
- ICX - 3

Color Legend:
- Blue line: SIP registration request
- Red line: Voice communication path
- Yellow line: Future SIP trunk
- Green line: TDM connection

Others ANS
## Which Reasons you need to SBC?

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality of Service</td>
<td>Call admission control, routing, Billing, NAT</td>
</tr>
<tr>
<td>Security</td>
<td>Encryption, Authentication, Policy, Firewall, VoIP Fraud</td>
</tr>
<tr>
<td>Interoperability</td>
<td>SIP -SIP-1 H323-sip, DTMF relay and interworking, Voice Transcoding</td>
</tr>
<tr>
<td>Demarcation</td>
<td>Fault Isolation, Topology Hiding, Session Border</td>
</tr>
</tbody>
</table>
Call Admission Control

- Check available Bandwidth
- Congestion Control
- CAC rejects calls when either there is insufficient CPU processing power
Routing Control

- Class 4 routing:
- Internal Routed database
- Load share Database
- Priority routing
- Least cost routing
- Or custom routing

- Radius AAA
- Authentication, Authorization,
- Accounting

Billing and Routing
Session Troubleshooting

- Live call analysis
- Call test
- Call recording
- Live wireshark analysis
SBC Demarcation

Demarcation
1. Fault Isolation and dynamic black list
2. Topology hiding
SBC Security

Threat Protection

UDP Threats
- UDP Flood
- RTP Threats
  - RTP spoofing
SIP Threats
- SIP Invite spoofing
- IP Threat
- IP Spoofing
- ICMP Threat
  - ICMP flood
- TCP Threat
  - Scan attack
  - TCP port

Sip firewall

Log or block failed sip request

IP firewall

Block service
Allow service

SBC Intrusion Detection

SBC has been pre-configured with a set of known attacks

Sip rate limit

Prevent DOS type attack
If limit cross Dynamic block IP
Segment of VoIP Security

Layer 3 attack
Layer 4 attack

OS attack
Application attack

SIP protocol fuzzing
SIP denial of service/distributed denial of service
SIP spoofing
SIP advanced toll fraud (call walking, stealth attacks)

Media Replication
Signaling/Media Encryption

Firewall
IDS / IPS
SBCE Standard
SBCE Advanced
IP-PBX
SBC interoperability

Connect every call
1. Connect sessions even with miasmas
2. Less route retries call ASR increase
3. Connect session even no common codec
4. Establish more calls to improve ASR
SBC Cover your business size?

High capacity up to 60000 current session handle with media RTP

Swift handle inbound and outbound call

Minimize delay on call setup

Reduce call drop
THE WEAPONS AT THEIR FINGERTIPS

10,000 BC: Prehistoric weapons

10 BC: Rome vs. Carthage

1500 AD: Knights vs. Musketeers

1910 AD: World War I

2010 AD: Drone Strike

TODAY: Cyber-Attack
Thank You