

# RED SHIFT

## NETWORKS

Type of Threat	Detailed Description
Eavesdropping	Eavesdropping attacks describe a method by which an attacker is able to monitor the entire signaling and/or data stream between two or more VoIP endpoints, but cannot or does not alter the data itself.
Call Pattern Tracking	<p>Call Pattern Tracking is the unauthorized analysis by any means of any traffic from or to any node or collection of nodes on the network. It includes monitoring and aggregation of traffic for any form of unauthorized pattern or signal analysis.</p> <p>Call Pattern Tracking is a technique for discovery of identity, affiliation, presence and usage. It is a general technique that enables unauthorized conduct such as theft, extortion and deceptive practices including phishing.</p>
Traffic Capture	Traffic Capture is the unauthorized recording of traffic by any means and includes packet recording, packet logging and packet snooping for unauthorized purposes. Traffic capture is a basic method for recording a communication without the consent of all the parties.
Number Harvesting	Number Harvesting is the unauthorized collection of IDs, which may be numbers, strings, URLs, email addresses, or other identifiers in any form which represent nodes, parties or entities on the network. Number Harvesting is an unauthorized means of capturing identity and enabling subsequent unauthorized communication, theft of information and other deceptive practices.
Control Packet Eavesdropping -- Conversation Eavesdropping and Analysis	Capture unencrypted identities, PINs, phone numbers, credit cards

CONFIDENTIAL

<p>Call Black Holing</p>	<p>Call Black Holing (also known as "call blackholing") is any unauthorized method of dropping, absorbing or refusing to pass IP or another essential element in any VoIP protocol which has the effect of preventing or terminating a communication. Call Black Holing is defined to include any VoIP protocol for any form of communication, whether voice only or converged with other media including video, text and images.</p>
<p>Call rerouting (redirect poison)</p>	<p>Call Rerouting (also known as "call sinkholing") is any method of unauthorized redirecting of an IP or other essential element of any VoIP protocol with the effect of diverting communication. A consequence of Call Rerouting is to include unauthorized nodes, corresponding to unauthorized parties or other entities, into a communication.</p>
<p>Conversation Degrading</p>	<p>Conversation Degrading is the unauthorized and intentional reduction in quality of service (QoS) of any communication. Conversation Degrading is a method of attack on QoS that limits or frustrates communication. Unauthorized Degrading does not include lawful reductions in quality of service by the owners or operators of a communication system essential for network management.</p>
<p>Conversation Impersonation and Hijacking</p>	<p>Conversation Impersonation and Hijacking is the injection, deletion, addition, removal, substitution, replacement or other modification of any portion of any communication with information which alters any of its content and/or the identity, presence or status of any of its parties. Conversation Impersonation and Hijacking is a method of attack that applies to any communication including anyvoice, video, text and/or imaging data however encapsulated or encoded.</p>
<p>False Caller Identification</p>	<p>False Caller Identification is the signaling of an untrue identity or presence.</p>
<p>ARP Poisoning</p>	<p>Attacker is able to trick one or both hosts into thinking that the attacker's MAC address is the address of the other computer or of a critical server (SIP proxy, DNS server, and so on). As a result, attacker acts as a gateway (MITM), silently sniffing all traffic while forwarding it on to the intended host, all unknown to the victim)</p>

CONFIDENTIAL

Call Conference Abuse	Call Conference Abuse is an abuse of a VoIP call service as a means to hide identity for the purpose of committing fraud.
Call Stealing -- Toll Fraud	Attacker steals IP-PBX call minutes illegitimately and then sells into the black market
Premium Rate Service Fraud	Premium Rate Service Fraud is a method of artificially increasing traffic without consent or purpose other than to maximize billing.
Call bypass Connection via conf, signaling and transfer	Various forms of call bypass connection via conferencing, signaling and transferring means to add unauthorized parties, possibly dropping connections to conceal the fraud.
Call bypass Connection via conf, signaling and transfer	Various forms of call bypass connection via conferencing, signaling and transferring means to add unauthorized parties, possibly dropping connections to conceal the fraud.
Internal fraud exploiting internal access	Various forms of internal fraud exploiting internal access into authentication systems (e.g. RADIUS, LDAP, Active Directory, VOIP gateway and signaling switches).
Registration attacks	Registration attacks in which an attacker exploits vulnerabilities in registration injecting themselves into a signal path.
User Call Flooding	A DoS attack on a user, carried out by sending a large number of valid requests. While the associated Endpoint is able to process the requests, the user is continually interrupted.
User Call Flooding overflow to other devices	A DoS attack on a user, carried out by sending a large number of valid requests. While the associated Endpoint is able to process the requests, the user is continually interrupted. The difference from the previous case is that some of these calls may overflow to other resources including voice mail servers or call gateways whose resources may be exhausted.

CONFIDENTIAL

<p>Endpoint Request Flooding</p>	<p>A DoS attack on an Endpoint could consist of sending large number of valid/invalid call set up messages (e.g., SIP INVITEs) which could cause the Endpoint to crash, reboot, or exhaust all Endpoint resources including that of the User Agent. This may be observable by the end user, as some of the requests will be result in valid call setups. This type of attack can also impact the Call Processor if the attack is launched in such manner that it arrives from the PSTN.</p>
<p>Endpoint Request Flooding after Call Setup</p>	<p>A DoS attack on an Endpoint could consists of sending a large number of valid/invalid call control messages (e.g., SIP RE-INVITEs) after a call has been successfully established which could cause the Endpoint to crash, reboot, or exhaust all Endpoint resources. This may also result in dropping the existing connection.</p>
<p>Call Controller Flooding</p>	<p>A DoS attack to a Call Controller could consists of sending a large number of valid/invalid call set up messages (e.g., SIP INVITEs) which could cause the Call Controller to crash, reboot, or exhaust all call controller resources. This can affect a large number of Endpoints at one stroke, leaving them unable to initiate or receive calls.</p>
<p>Request Looping</p>	<p>A DoS attack may exploit loop and spiral implementation on a Call Controller to have two Endpoints across domains or within the domain continually forwarding a single request message, back and forth, to each other so as to exhaust resources on the Call Controller. This can affect a large number of Endpoints at one stroke, leaving them unable to initiate or receive calls.</p>
<p>Directory Service Flooding</p>	<p>A DoS attack could consist of sending large number of valid queries to the on a support server providing a VoIP services such as a Directory Server, DHCP Server, DNS server, etc. This could cause the associated server to crash, reboot, or exhaust all processing resources. The Endpoints that rely on this service would then be taken out of service, unless there exists some sort of redundancy in place.</p>
<p>Dos on Signaling</p>	<p>All variations of DoS attacks using combinations of SIP signaling, INVITE, REINVITE, REGISTER, OPTIONS, NOTIFY floods</p>

CONFIDENTIAL

<p>Distributed DoS</p>	<p>In a distributed DoS attack, a large number – perhaps millions – of computers simultaneously generate traffic designed to exhaust network or application resources. The attack may be carried out in two stages, first infiltrating a hidden control program, or “stealth worm” into network-attached computers, and then using these controls to cause the infected computer to launch the actual DoS attack. The second stage of the attack might or might not involve any direct action by the attacker; the attack could easily be launched automatically at some pre-specified time.</p>
<p>Malformed Request and Message (Protocol Fuzzing)</p>	<p>The specifications for control messages in many VoIP implementations are deliberately open-ended, to allow for the addition of additional capabilities over time. The downside of this type of specification is that it is not possible to test an implementation either for correct processing of all valid messages or for accurate recognition of invalid messages. As a consequence, valid but complex messages are at risk of being discarded, and the processing systems themselves are at risk if they are sent sufficiently devious invalid messages. The ability of complex invalid messages both to be accepted by a call processing element and to trigger self-destructive behavior in that element creates the threat of DoS via “killer messages.”</p>
<p>Disabling Endpoint with invalid requests</p>	<p>A DoS attack on an Endpoint could consist of sending a number of invalid call setup messages (e.g., ACKs when none is expected) that could cause the Endpoint to crash, reboot, or exhaust all Endpoint resources including that of the User Agent. This may not be observable by the User Agent since a lower layer protocol processing engine would process and drop the messages. It is not always necessary to overload the Endpoint with the sheer volume of invalid messages. Unless the message is recognized as invalid and quickly discarded some invalid messages can consume a considerable amount of processing capacity, and they can corrupt the protocol processing engine by overflowing the message buffers.</p>
<p>Injecting invalid media into call processor</p>	<p>This form of DoS can be triggered by the injection of invalid media into the call processor by the caller or by a third party (by guessing the appropriate control headers of the media stream). This will cause the Endpoints to crash, reboot, or exhaust all call processing capacity.</p>

CONFIDENTIAL

<p>Malformed Protocol Messages</p>	<p>This form of attack consists of sending malformed signaling messages (messages with overflow or underflow). These messages are sent to the processing node degrading its performance resulting in its inability to process normal messages and setup and tear down calls. Fuzzing involves creating unanticipated types of packets for a protocol, which contain data that pushes the protocol's specifications to the point of breaking them. These packets are sent to a processing node that acts on the target protocol, to disable the processing node or degrade its performance (crash, resource consumption, etc.). A well known SIP public fuzzer is the PROTOS suite developed by the University of OULU in Finland.</p>
<p>QoS Abuse or QoS Modification</p>	<p>Quality of Service (QoS) abuse involves an attacker violating the QoS negotiated at setup. For example, it could use a different media coder than what was declared during call setup. It is also possible for data applications to encroach on or misuse the QoS defined for voice. This would have the effect of introduced latency which adversely affects voice quality during a call. Twiddle 802.1q or IP TOS bits to alter engineered QoS</p>