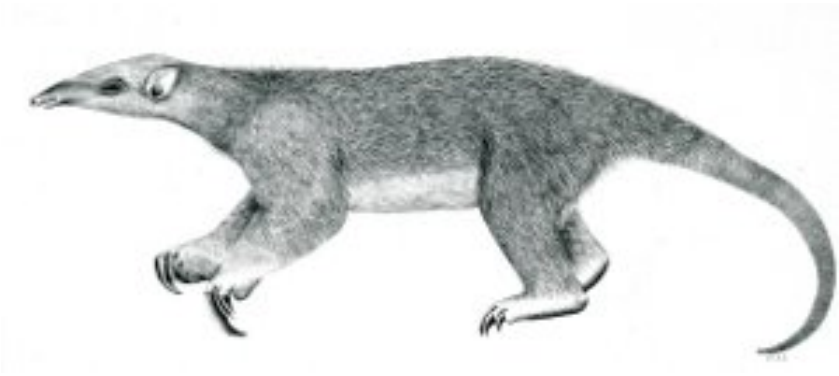
Tranalyzer2

voipDetector

VoIP



Tranalyzer Development Team

Contents

1 voipDetector

1.1 Description

The idea of this plugin is to identify SIP, RTP and RTCP flows independently of each other, so that also non standard traffic can be detected. Moreover certain QoS values are extracted.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Variable	Default	Description	Flags
VOIP_ANALEN	1	1: additional check report len against payload length 0: only ssrc check	
VOIP_V_SAVE	0	save rtp content to VOIP_RM_DIR	
VOIP_RM_DIR	0	rm RTP content directory	VOIP_V_SAVE=1
VOIP_PLDOFF	0	offset to payload pointer to save content	VOIP_V_SAVE=1
SIPNMMAX	40	maximal sip caller name length in flow file	
VOIP_PATH	"/tmp/"	default path of content directory	
VOIP_FNAME	"eier"	default content file name prefix	

1.3 Flow File Output

The voipDetector plugin outputs the following columns:

Column	Type	Description
voipStat	H16	Status
voipID	H32	RTP/RTCP ID
voipSRCnt	U8	RTP SID/RTCP record count
voipTyp	U8	RTP/RTCP type
voipPMCnt	U32	RTP packet miss count
voipPMr	F	RTP packet miss ratio
voipSIPStatCnt	U8	SIP stat count
voipSIPReqCnt	U8	SIP request count
voipSIPCID	S	SIP Call ID
voipSIPStat	R(U16)	SIP stat
voipSIPReq	R(S)	SIP request
voipTPCnt	U32	RTCP cumulated transmitter packet count
voipTBCnt	U32	RTCP cumulated transmitter byte count
voipCPMCnt	U32	RTCP cumulated packet miss count
voipMaxIAT	U32	RTCP maximal Inter Arrival Time

1.3.1 voipStat

The `voipStat` column is to be interpreted as follows:

voipStat	Name	Description
2^0 (=`0x0001`)	RTP	RTP detected
2^1 (=`0x0002`)	RTCP	RTCP detected
2^2 (=`0x0004`)	SIP	SIP detected
2^3 (=`0x0008`)	STUN	STUN present
2^4 (=`0x0010`)	X	RTP: extension header
2^5 (=`0x0020`)	P	RTP: padding present
2^6 (=`0x0040`)	-	-
2^7 (=`0x0080`)	M	RTP: data marker set
2^8 (=`0x0100`)	WROP	RTP: content write operation
2^9 (=`0x0200`)	-	-
2^{10} (=`0x0400`)	-	-
2^{11} (=`0x0800`)	-	-
2^{12} (=`0x1000`)	PKTLSS	RTP: packet loss detected
2^{13} (=`0x2000`)	RTPNFRM	RTP: new frame header flag
2^{14} (=`0x4000`)	-	-
2^{15} (=`0x8000`)	-	-

1.4 TODO

- Skype
- Google Talk