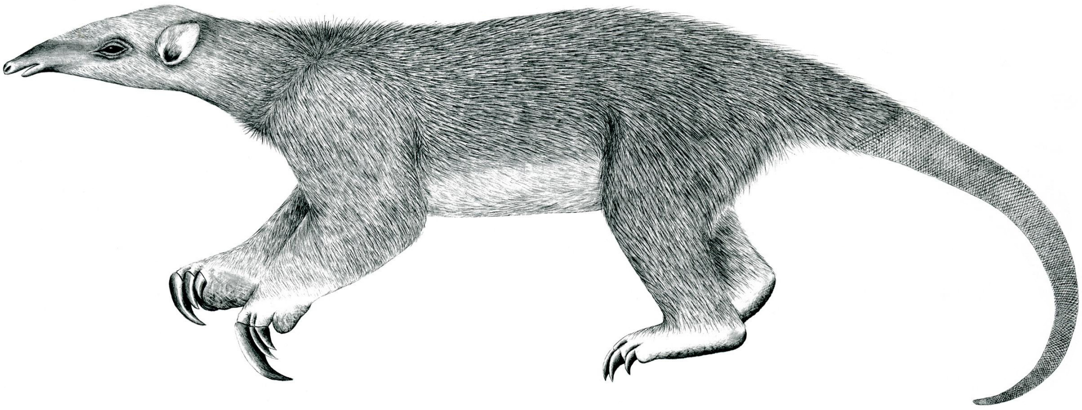
Tranalyzer2

voipDetector

Voice over IP (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:

Name	Default	Description	Flags
VOIP_SIP	2	0: do not decode SIP, 1: Enable SIP decoder, 2: Decode SIP and add RTP/SIP findex/ssrc flow correlation	
VOIP_SIP_PRV	0	0: No RTP/SIP flow correlation enhancement, 1: add RTP srcIP, 2: add srcIP of SIP flow	VOIP_SIP=2 VOIP_SIP=2 VOIP_SIP=2
VOIP_RTP	1	Enable RTP decoder	
VOIP_RTCP	1	Enable RTCP decoder	
VOIP_ANALEN	0	0: only ssrc check, 1: additional check report len against payload length	
VOIP_SAVE	0	Save RTP content to VOIP_V_PATH	
VOIP_BUFMODE	1	Enable buffering of saved RTP content	VOIP_SAVE=1
VOIP_SILREST	1	Restore back G.711 suppressed silences	VOIP_SAVE=1
VOIP_PLDOFF	0	Offset for payload to save	VOIP_SAVE=1
VOIP_SVFDX	1	Merge ops: 1: findex, 0: SSRC	VOIP_SAVE=1
VOIP_MINPKT	1	Minimum packet length of a flow	VOIP_SAVE=1

RTPFMAX	10	Maximal SSRC files	VOIP_SAVE=1&&
			VOIP_SVFDX=0

SIPNMMAX	35	Maximal SIP caller name length	
SIPSTATMAX	8	Maximal SIP state requests	
SIPCLMAX	3	Maximal SIP state requests name length	
SIPRFXMAX	100	Maximal SIP IP, m=audio / video ports	
RTPBUFSIZE	4096	Size of buffer for RTP content	VOIP_SAVE=1
RTPMAXVERS	1	Maximal number of version violations	
VOIP_RMDIR	1	Empty VOIP_V_PATH before starting	VOIP_SAVE=1
VOIP_PERM	S_IRWXU	File permissions	VOIP_SAVE=1
VOIP_V_PATH	"/tmp/TranVoIP"	Path for extracted content	VOIP_SAVE=1
VOIP_FNAME	"nudel"	Default content file name prefix	VOIP_SAVE=1

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- VOIP_RMDIR
- VOIP_V_PATH

- VOIP_FNAME

1.3 Flow File Output

The voipDetector plugin outputs the following columns:

Column	Type	Description	Flags
voipStat	H16	Status	
voipType	R(U8)	RTP/RTCP type	
voipSSRC	R(H32)	RTP/RTCP Synchronization Source Identifier	
voipCSRC	R(H32)	RTP/RTCP Contributing Sources	
voipSRCnt	U8	RTP SID / RTCP record count	
rtpPMCnt	U32	RTP packet miss count	
rtpPMr	F	RTP packet miss ratio	
sipMethods	H16	SIP methods	VOIP_SIP>0
sipStatCnt	U8	SIP stat count	VOIP_SIP>0
sipReqCnt	U8	SIP request count	VOIP_SIP>0
sipUsrAgnt	S	SIP User-Agent	VOIP_SIP>0
sipRealIP	S	SIP X-Real-IP	VOIP_SIP>0
sipFrom	R(S)	SIP Caller	VOIP_SIP>0
sipTo	R(S)	SIP Callee	VOIP_SIP>0
sipCallID	R(S)	SIP Call-ID	VOIP_SIP>0
sipContact	R(S)	SIP Contact	VOIP_SIP>0
sipStat	R(U16)	SIP stat	VOIP_SIP>0
sipReq	R(SC)	SIP request	VOIP_SIP>0
sdpSessID	R(S)	SDP session ID	VOIP_SIP>0
sdpRFAdd	R(IP)	SDP RTP audio/video flow address	VOIP_SIP>0
sdpRAFPrt	R(U16)	SDP RTP audio flow port	VOIP_SIP>0
sdpRVFPrt	R(U16)	SDP RTP video flow port	VOIP_SIP>0
sdpRTPMap	R(SC)	SDP rtpmap	VOIP_SIP>0
voipFindex	R(U64)	SIP RTP findex	VOIP_SIP>1
rtcpTPCnt	U32	RTCP cumulated transmitter packet count	VOIP_RTCP=1
rtcpTBCnt	U32	RTCP cumulated transmitter byte count	VOIP_RTCP=1
rtcpFracLst	U8	RTCP cumulated fraction lost	VOIP_RTCP=1
rtcpCPMCnt	U32	RTCP cumulated packet miss count	VOIP_RTCP=1
rtcpMaxIAT	U32	RTCP max inter-arrival time	VOIP_RTCP=1
voipFname	S	RTP content filename	VOIP_SAVE=1

1.3.1 voipStat

The voipStat column is to be interpreted as follows:

voipStat	Description
2^0 (=0x0001)	RTP detected
2^1 (=0x0002)	RTCP detected
2^2 (=0x0004)	SIP detected
2^3 (=0x0008)	STUN detected
2^4 (=0x0010)	RTP extension header
2^5 (=0x0020)	RT(C)P padding bytes
2^6 (=0x0040)	SDP detected
2^7 (=0x0080)	RTP marker
2^8 (=0x0100)	RTP content write operation
2^9 (=0x0200)	SIP audio RTP flow announced
2^{10} (=0x0400)	SIP video RTP flow announced
2^{11} (=0x0800)	sdpRFAdd field truncated… increase SIPRFXMAX
2^{12} (=0x1000)	RTP packet loss detected
2^{13} (=0x2000)	RTP sequence number jump to past
2^{14} (=0x4000)	RTP new frame header flag
2^{15} (=0x8000)	RTP error in detection

1.3.2 sipMethods

The sipMethods column is to be interpreted as follows:

sipMethods	Description
2^0 (=0x0001)	Unknown method
2^1 (=0x0002)	INVITE
2^2 (=0x0004)	ACK
2^3 (=0x0008)	BYE
2^4 (=0x0010)	CANCEL
2^5 (=0x0020)	REGISTER
2^6 (=0x0040)	OPTIONS
2^7 (=0x0080)	PRACK
2^8 (=0x0100)	SUBSCRIBE
2^9 (=0x0200)	NOTIFY
2^{10} (=0x0400)	PUBLISH
2^{11} (=0x0800)	INFO
2^{12} (=0x1000)	REFER
2^{13} (=0x2000)	MESSAGE
2^{14} (=0x4000)	UPDATE
2^{15} (=0x8000)	—

1.4 Packet File Output

In packet mode (-s option), the voipDetector plugin outputs the following columns:

Column	Type	Description	Flags
voipStat	H16	Status	
voipType	R(U8)	RTP / RTCP type	
voipSeqN	U8	RTP / RTCP sequence number	
voipTs	U32	RTP / RTCP timestamp	
voipTsDiff	I32	RTP / RTCP timestamp difference	
voipSSRC	H32	RTP / RTCP ID	

1.5 Monitoring Output

In monitoring mode, the voipDetector plugin outputs the following columns:

Column	Type	Description	Flags
voipFHndl	U64	Number of file handles	VOIP_SAVE=1
sipPkts	U64	Number of SIP packets	VOIP_SIP>0
sipUnkPkts	U64	Number of SIP UNKNOWN packets	VOIP_SIP>0
sipInvPkts	U64	Number of SIP INVITE packets	VOIP_SIP>0
sipAckPkts	U64	Number of SIP ACK packets	VOIP_SIP>0
sipByePkts	U64	Number of SIP BYE packets	VOIP_SIP>0
sipCanPkts	U64	Number of SIP CANCEL packets	VOIP_SIP>0
sipRegPkts	U64	Number of SIP REGISTER packets	VOIP_SIP>0
sipOptPkts	U64	Number of SIP OPTIONS packets	VOIP_SIP>0
sipPraPkts	U64	Number of SIP PRACK packets	VOIP_SIP>0
sipSubPkts	U64	Number of SIP SUBSCRIBE packets	VOIP_SIP>0
sipNotPkts	U64	Number of SIP NOTIFY packets	VOIP_SIP>0
sipPubPkts	U64	Number of SIP PUBLISH packets	VOIP_SIP>0
sipInfPkts	U64	Number of SIP INFO packets	VOIP_SIP>0
sipRefPkts	U64	Number of SIP REFER packets	VOIP_SIP>0
sipMsgPkts	U64	Number of SIP MESSAGE packets	VOIP_SIP>0
sipUpdPkts	U64	Number of SIP UPDATE packets	VOIP_SIP>0
sdpPkts	U64	Number of SDP packets	VOIP_SIP>0
sipAPCnt	U64	Number of unique SDP audio address, port	VOIP_SIP>0
sipFdxMtch	U64	Number of SIP/RTP matches	VOIP_SIP>0
rtpPkts	U64	Number of RTP packets	VOIP_RTP=1
rtcpPkts	U64	Number of RTCP packets	VOIP_RTCP=1

1.6 Plugin Report Output

The following information is reported:

- Aggregated voipStat
- Aggregated sipMethods

- Number of SIP packets (`VOIP_SIP=1`)
- Number of SIP UNKNOWN packets (`VOIP_SIP=1`)
- Number of SIP INVITE packets (`VOIP_SIP=1`)
- Number of SIP ACK packets (`VOIP_SIP=1`)
- Number of SIP BYE packets (`VOIP_SIP=1`)
- Number of SIP CANCEL packets (`VOIP_SIP=1`)
- Number of SIP REGISTER packets (`VOIP_SIP=1`)
- Number of SIP OPTIONS packets (`VOIP_SIP=1`)
- Number of SIP PRACK packets (`VOIP_SIP=1`)
- Number of SIP SUBSCRIBE packets (`VOIP_SIP=1`)
- Number of SIP NOTIFY packets (`VOIP_SIP=1`)
- Number of SIP PUBLISH packets (`VOIP_SIP=1`)
- Number of SIP INFO packets (`VOIP_SIP=1`)
- Number of SIP REFER packets (`VOIP_SIP=1`)
- Number of SIP MESSAGE packets (`VOIP_SIP=1`)
- Number of SIP UPDATE packets (`VOIP_SIP=1`)
- Number of SDP packets (`VOIP_SIP=1`)
- Number of unique SDP audio address, port (`VOIP_SIP=1`)
- Number of unique SIP/RTP flow matches (`VOIP_SIP=1`)
- Number of RTP packets (`VOIP_RTP=1`)
- Number of RTCP packets (`VOIP_RTCP=1`)
- Max number of file handles (`VOIP_SAVE=1`)

1.7 TODO

- Skype
- Google Talk