The RTP bleed and what can we do?

4 February 2018

Peter Lemenkov
Software Engineer, Red Hat

What is it and how it affects us?

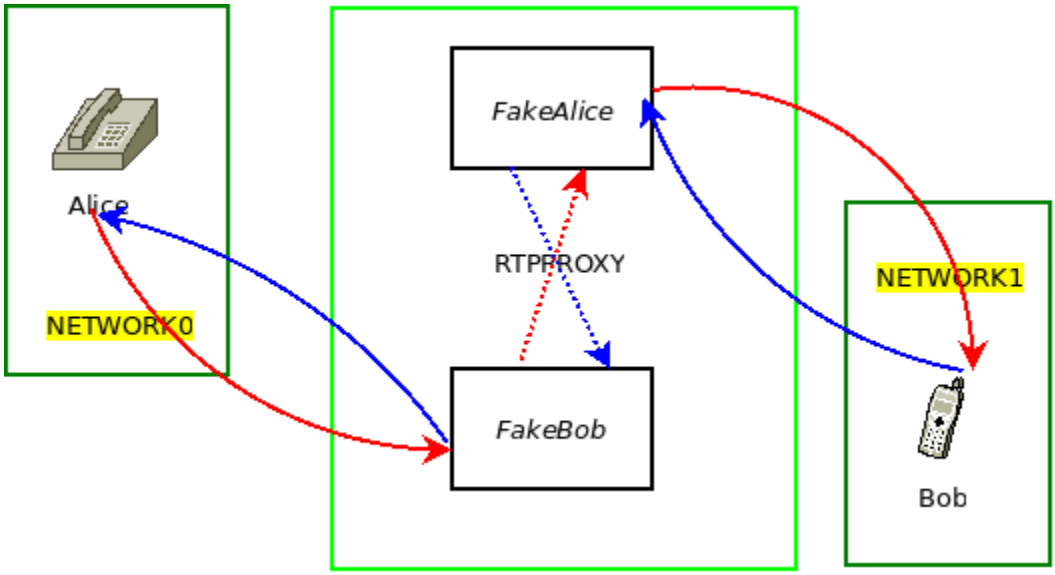
- The RTP bleed (https://www.rtpbleed.com) intially made public by Sandro Gauci (https://twitter.com/sandrogauci) and Klaus-Peter Junghanns (https://github.com/kapejod)
- Allows almost anyone to redirect media streams.
- Cannot be mitigated in 100% cases

POTS RTP bleed

Why it was introduced in the first place?

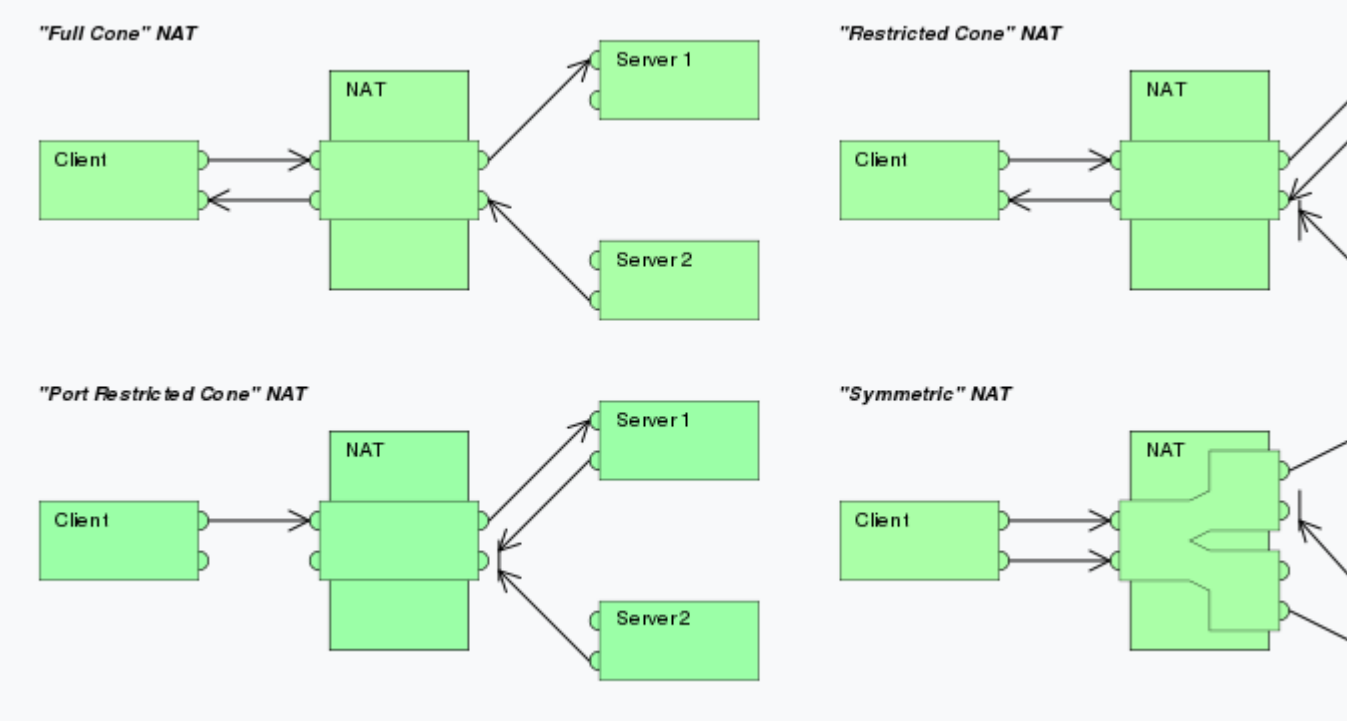
- Lots of legacy with poor security
- We have to deal with NAT somehow

RTP proxying



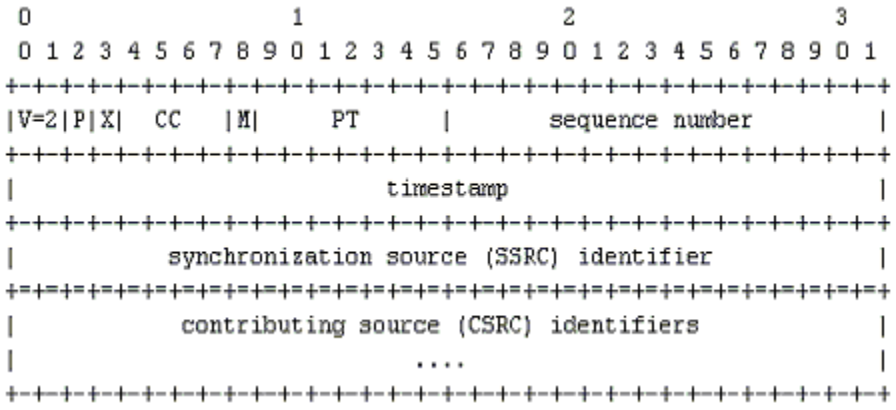
- Multiple implementations
- Most simple case - there are more (transcoding, etc).
- RTP proxy is visible to both callers
- RTP proxy allocateis ports and resends data to calling parties
- Who actually sends data to these ports? The same question as in POTS.

Avoid RTP proxying with STUN?



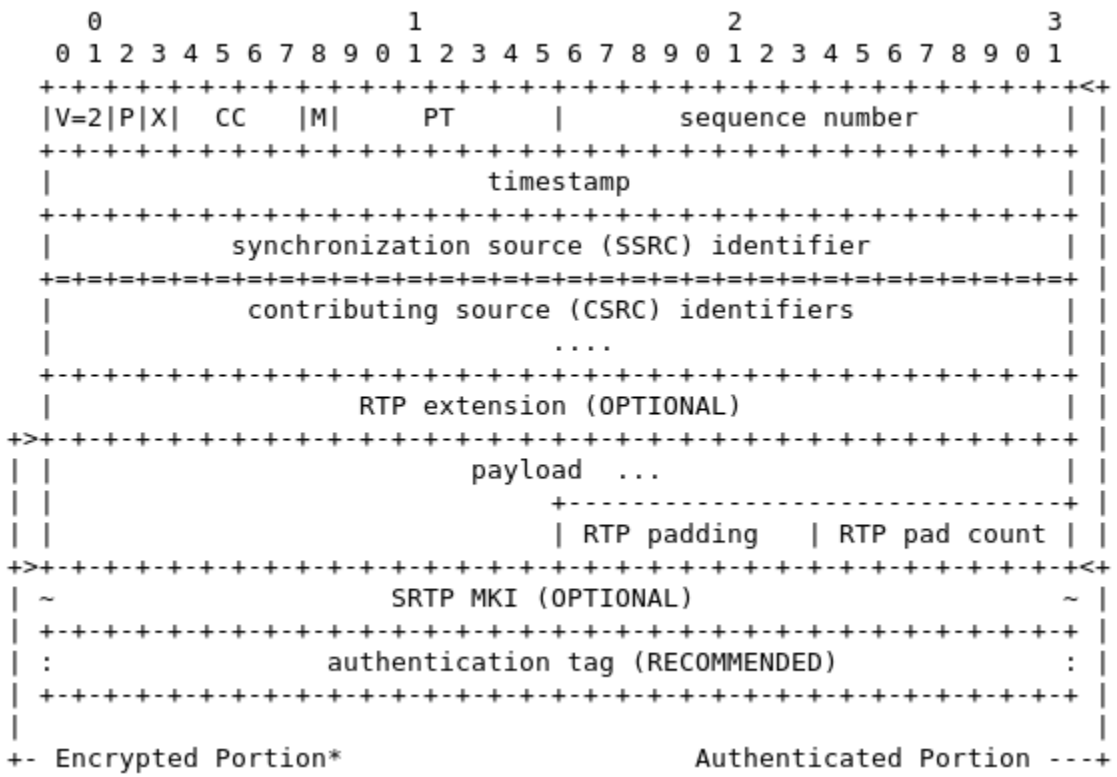
- No.

RTP structure



- That's all we have.

SRTP structure



- Extends RTP with authentication

What can we do to mitigate it using current architecture?

- In short - we can't do much
- Remembering last IP? Doesn't work with 4G networks
- SSRC also could change although this looks to be rare
- No signature of any kind
- Even if possible to "sign" (SRTP), then what to do with legacy devices?

Will future Voice / Video over IP systems be affected?

- IPv6
- ***Encryption*** (SRTP + MIKEY, ZRTP, SDES, DTLS-SRTP)

Thank you

Peter Lemenkov
Software Engineer, Red Hat
lemenkov@gmail.com (mailto:lemenkov@gmail.com)
https://github.com/lemenkov (https://github.com/lemenkov)