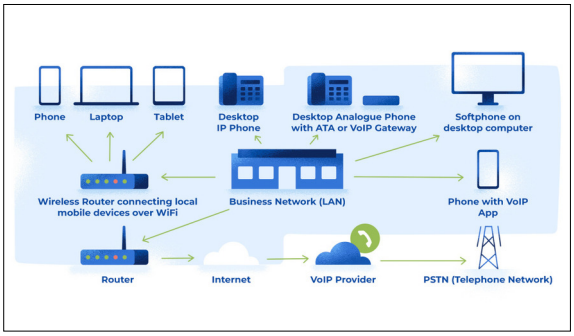

Michel Bongard

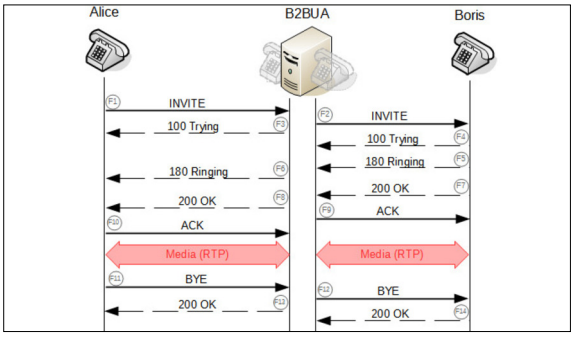

Dominique Illi

Students	Michel Bongard, Dominique Illi
Examiner	Cyrill Brunschwiler
Subject Area	Networks, Security & Cloud Infrastructure

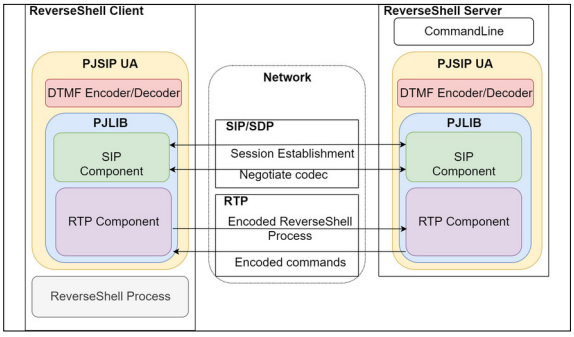
Reverse Shell via Voice (SIP, Skype)



How VoIP works
https://www.nextiva.com/blog/what-is-voip.html



SIP session establishment
https://www.wikiwand.com/en/Session_Initiation_Protocol



Reverse shell over VoIP - System overview
Own presentment

Initial Situation: Nowadays, there are less and less points of entry for a hacker to attack a network. Modern network infrastructures are specifically designed to deny any attempt of direct access from the Internet into an internal network. To circumvent those restrictions, it is often easier to initiate a data-channel from within the internal network.
There already exist ways to establish such inside out channels such as the TCP reverse shell. However, most of these attacks are not very difficult to detect by network intrusion detection systems.
One alternative is the encapsulation of payload inside VoIP packets. This thesis is a feasibility study featuring a proof of concept providing a reverse shell over VoIP.

Approach / Technology: Due to the popularity of SIP and Skype, this thesis focuses on these two VoIP protocols. First, a thorough understanding of both protocols had to be acquired. After an initial research phase, the decision was made to develop the proof of concept for SIP. SIP is open source and existing libraries can be used as a foundation. Skype's proprietary nature would require reverse engineering the protocol.
In the final proof of concept, the open source C-library “PJSIP” is used. PJSIP included sample user agents that were left largely untouched, so that a normal SIP session can get established.
The attacker then encodes a shell command to audio using a mapping between the ASCII table and different audio frequencies. The audio is placed inside RTP packets and transmitted to the victim. There, the audio gets converted back to text and the shell command is executed. The resulting output is sent back to the attacker using the same scheme.

Result: This thesis proofed that a reverse shell over VoIP is feasible.
At the moment it works only when both attacker and victim are in the same network. To make the solution work over the Internet as well, UDP packet loss needs to be handled.
However, when both clients are in the same LAN, a reverse shell can be established between the victim and the attacker, allowing the attacker to execute arbitrary commands on the victim's client at the very low rate of 50 bytes per second. Nonetheless, as the transmission is based on audio, it would also work if SIP Gateways send the tunnel traffic over plain-old telephony networks (POTS).