Security Flaws in VPN-Project Implementation

Comments regarding the security flaws and potential exploits of the VPN architecture.

Hannes Rabo
School of Electrical Engineering and Computer Science
KTH - Royal Institute of Technology
hannes.rabo@gmail.com

I. Introduction

In this short report, two security flaws in the implementation of the VPN project are briefly presented and discussed together with solutions.

II. Redirection vulnerabilities in the Handshake

In the handshake between client and server, it is a possible that a malicious alters the target message from the client and select their own computer as a final destination for the VPN server. This means that when the user communicates with the VPN client, the traffic will go to the malicious user instead of the secure application behind a firewall as intended. To prevent this from happening, the handshake needs a signed cryptographic hash of all handshake messages in the end. Any alterations to the settings would invalidate the hash and any alterations to the hash could not be signed by client private key.

III. Replacing VPN Client-Session

With the same reasoning as the attack described above, it is also possible to inject a TCP packet to replace the server's ”Session” message. In this case the session key, session IV, server port and server host could be replaced with a machined controlled by the attacker which completely bypasses the real VPN server. As the client never performs any integrity checks of the information, this would allow an attacker to completely take control of the session with the VPN client. The same type of solution as mentioned above is applicable to this problem.