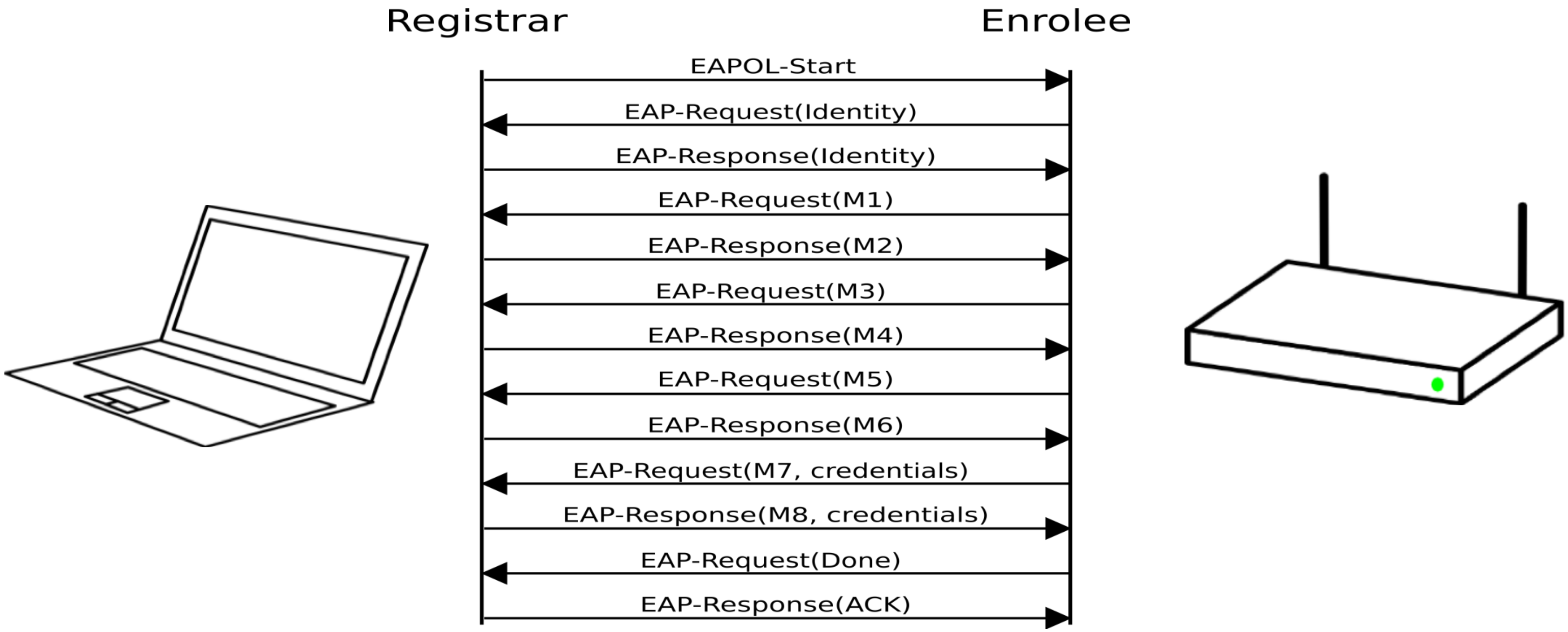

-So all we need to do it find the seed (x)! Some sources say that the seed may be the router's uptime (very poor design broadcom!)

-This may not be true, but if it is, we just use MDK3 or deauth the router until the owner reboots it, that makes our seed a very low number!

-Easy to guess seed=easy to brute force. Maybe it could even be a process ID? I don't know, we have to understand the generator from the source.

-So we toss in a seed (hopefully its one of the two options I just suggested) then just check to see if we get a matching PKE nonce.

-Once we know that, we can just use the code wiire wrote and input the data (PKE, PKR, E-S1, E-S2, E-Hash1, E-Hash2) and then brute force the pin the same exact way he does.

-The only thing I don't understand is the Authkey. I'll wait for wiire or another guy I'm talking to to help =D