Default WiFi password generation using PUFs

Default WiFi passwords on routers are one of the weakest links in the overall security of the network. Usually, people don't change the default WiFi password. Companies such as TP-LINK, use last 10 digits of the MAC address as the default WiFi password on some of their devices, which makes it very easy for the attacker to get inside the network.

Our Idea is to use uninitialized memory as a PUF on these routers. In our approach, we will use the uninitialized memory of a device peripheral, such as the wireless module. Using a PUF implemented on a device peripheral instead of the system's memory will give us the advantage, that we can verify the PUF response without restarting the device. It will also enable us to implement the default WiFi password using PUFs to existing devices without modifying their firmware/bootloader. We only need a user-space program to access this PUF. Such a PUF can be used to create a unique secret, which will be used as a default password for WiFi.

For the implementation of such a system, we need to develop a program which can read the uninitialized memory from the device peripherals such as WiFi module and generates a deterministic secret from it. Then this program needs to access WiFi management API in Linux and set the WiFi password to the generated secret. We need to package the binary of the program in the Linux init-disk and we need to add this program as a startup program in the init script. A configuration file is also needed to track that a system is booting for the first time so that the program will only set the default WiFi password on the first boot.

We can then make a complete firmware including our modification of the Linux image. An administrator who will install this firmware on a new device can view the password set by the program and print it out on the device for the end-user. We can also extend this idea to generate strong password using a combination of user input and the secret generated by the PUF response. This will help the end-user to generate a strong new passwords if they want to change the default one.