Continuation packets...can send as many as we want so can we send data to an address with a continuation packet…

Since all packets are broadcasted can I create a device that listens on every frequency?

Shared key…how do we get the devices to reshare the key?

Attack vectors in a typical BTLE attack:

Key sniffing

Replay attack

Actual application

Hardware

MCUs:

Nordic NRF51822

MSP430

MITM proxy yourself

Application level:

Air BnB locks:

Can set time that users can use lock but there is a possibility to mitm and change time we are allowed to use the lock. From own device

With low energy comes low security.

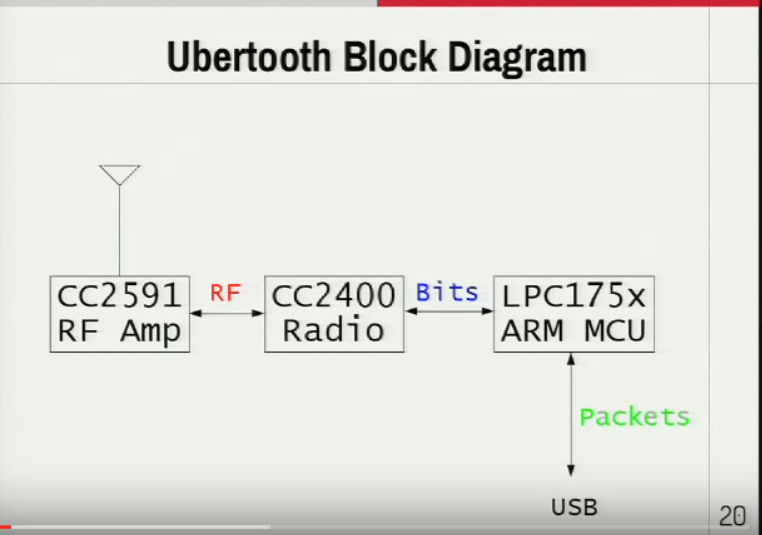
Paper about the Noke

<https://blog.ssdev.org/?p=3299>

<http://www.javadecompilers.com/apk>

<http://blogmal.42.org/rev-eng/patching-android-apps.story>

<https://www.youtube.com/watch?v=Mo-FsEmaqpo>



<https://www.youtube.com/watch?v=Mo-FsEmaqpo>

Connect packet contains Access Address, Hop parameters, and CRC Init.

Promiscuous Mode:

See an empty packet (14 bits: 1 with 13 0’s) then rewind 32 bits and we have a potential access address. After seeing that access address “enough times” then assume it is a valid access address.

Recovering CRCInit:

Filter packets by Access Address

Plug CRC into LFSR and run it backward

Once we have seen it a couple times then we assume it is the CRC.

Recovering Hop Interval:

Observation: 37 is prime; sit on data channel and wait for two consecutive packets delta t/37 = hop interval (except assumes that it is using every channel)