Vychazim z predpokladu, ze ten Bonega telegram co se nachazi v DP KZ, je zachyceny nejakym tim Vasim USB snifferem, tak jak je zapsan v praci ci v danem PPT.

Zjsitil jsem, ze bud

* Ja mozna plne nechapu specifikaci sifrovaneho wm-bus prenosu. Mam za to, ze Sniffer by mel zachytit sifrovany paket, tak jak ho vysle METER, ja si spocitam inicializacni vektor, vezmu AES klic daného zarizeni a provedu desifovani. Pokud zachytim snifferem telegramu vice zarizeni, provedu stejne pro kazde zvlast (vlastní IV i KEY).
* V UniPi nedomysleli nasazeni RasPi jako MUCu a zvolili první cip wmbus cip co se namanul, aniz by poradne procetli specifikaci nebo to odzkouseli.
* V IQRF jsou strasne vizionářští. Pocitaji vicemene s tim, ze jejich cipy budou slouzit primarne jako METERy. Specifikace je tomu prizpusobena, zatímco MUC je pouze experiental. A je tak experimental, ze ma umelou inteligenci. Nebo ja jsem dement.

Protoze,

1. zvoleny IQRF cip umoznuje do EEPROMky zapisovat AES klic a vlastne všechny hodnoty C,M,A pole. To je celkem pochopitelne pro nasazeni jako METER.
2. Jenze on ten AES klic pouziva i v modech prijmu (MUC, Sniffer) a DESIFRUJE s nim AUTOMATICKY všechny prijmane sifrovane pakety. Takze to co vidi sniffer (co vlastne vidim/zachytavam ja), je uz desifrovane tim klicem z EEPROM a je uplne jedno, jestli odpovida danemu paketu nebo ne (viz ta PPT co jsem posilal).
   1. Pokud klic odpovida, tak to vraci rozsifrovane a ja vlastne UZ PŘI PRIJMU dostavam rozsiforvana data a kdybych nevedel ze to je nastavene na AES, tak to nepoznam.
   2. Pokud klic neodpovida, prichazeji nejka zasifrovana data, která se nedaji pomoci sifrovaciho klice daného zarizeni rozšifrovat (viz ten muj problém s Bonegou popsany v tom PPT). Da se to ale „rozšifrovat“ tim klicem z IQRF, ale bohužel jen do podoby puvodne prenasenych sifrovanych dat.

Napada me sekvence reseni:

1. Pokud dobre chápu DP KZ, mate k dispozici 4 zarizeni, z cehoz dve AES neumi (ZPA, Pikkerton), u jednoho jde vypnout (Weptech), ale u jednoho je nutne (Bonega). Potom je tedy moznost nastavit do IQRF natvrdo klic od Bonegy. Takze všechna 4 zarizeni se nam budou prijimat nesifrovane. Ale to vlastne vuci UniPi neresi nic.
2. Vime jakym klicem (tim nastavenym v IQRF) jsou desifrovany veskere prichozi AES telegramy a ze sifra AES je symetricka. Tudiz se muze udelat workaround ve stylu:
   1. Prisla nam citelna nesifrovana data -> No problem -> Parsujme je.
   2. Prisla nam nejaka rozsifrovana data, ale nesedi kontrolni AES/CRC/whatever bajty -> Jsou to puvodne sifrovana data, ale jsou blbe rozsifrovana. Takze je vezmeme a zasifrujeme je zpatky univerzalnim klicem, kterým byla i blbe rozsifrovana (IQRF klic), tim ziskame puvodni sifrovana data „tak jak sla vzduchem“. Ted na tedy aplikujeme desifrovani AES prislusnym klicem (samotny klic zarizeni ) a prislusnym IV (ten umíme slozit). A zde získáváme rozsifrovana spravna data. -> Parsujeme. Nevyhodou je, ze proces se tim znacne komplikuje, bude to nachylnejsi na selhani/moznost chyby a uplne univerzalni to taky nebude. A je to reseni tak trochu na pytel. Ale asi jedine aktualne vyuzitelne. Vyhoda je, ze ten IQRF klic si muzeme dynamicky menit, zvýšíme tim bezpečnost prenosu :D
3. Pockame az IQRF doladi MUC mod. Potom by se snad dalo zmenit klic při kazdem synchronim dotazu. Jenze to narazi na problémy:
   1. Nelze rict, kdy to dodělají a jestli vůbec.
   2. Jestli nam ty zarizeni vubec zvladnou T2?
   3. Nejsem tedy schopen to otestovat a aktualne to taky nic neresi.
4. Vybodneme se na sifrovani. Coz poradne taky nic neresi a taky se pripravime o moznost vycitat Bonegy.