Suuri suunnitelma fobien suhteen

Tämä on tekninen dokumentti ja koskee lähinnä kuvion implementoijia, muut voivat mielenkiinnosta lukea mutta jos on kommentteja tai kysymyksia niin esitä ne IRCissä rambolle ja distille.

Alkuun lähinnä ulko-oven solenoidilukkoon, tulevaisuudessa voisi kuitata fobilla sähköt päälle työpisteeseen/-koneeseen.

Ref: http://kirjoitusalusta.fi/hacklab-uudet-tilat-2014

Lukkorunko:

- Arvolukko ehdottaa: EL580 (jaettu kara), avainpesä CYO37C CR.
    - ~820 asennettuna (kaiken oheissälän kera)

Kortti/fobi: Mifare DESFire EV1

Lukijat PN532, vaihtoehtoja:

- http://www.seeedstudio.com/depot/NFC-Shield-V20-p-1370.html
    - saapunut koeponnistukseen
- http://www.seeedstudio.com/depot/Xadow-NFC-p-1627.html
    - http://www.seeedstudio.com/depot/Xadow-Breakout-p-1519.html
        - ~~Ei välttämätön, lukijan piirin alla on padit joihin saa kolvattua johdot.~~
            - Ei saa kaikkia tarvittavia johtoja...
    - Saatu toimimaan BeagleBonella SPI:n yli
- https://www.adafruit.com/products/789
    - dist tietää hyväks (ja on mukana)
        - Saatu toimimaan raspilla UARTin yli
- http://www.seeedstudio.com/wiki/NFC_Shield_V1.0
    - Wanhentunut malli mutta juuri nyt kädessä
        - Saatu toimimaan raspilla SPI:n yli
- http://imall.iteadstudio.com/rdm8800-nfc-rfid-module.html
    - Vois olla kokeilemisen arvoinne
- http://imall.iteadstudio.com/im130625002.html
    - Kuten myös

"Tiedostojärjestelmä":

- Dummyapp vakioavaimella
    - Sessioiden avaamista varten

- HacklabApp
    - Kopio kortin UID:stä (voidaan varmentaa että kukaan ei yritä feikata kortin anonyymisti luettavaa UID:tä)
        - Tai joku muu UID, mutta sitten nämä molemmat pitää olla jäsenkannassa
    - Jäsennumero ??
    - muuta ??
    - Salattu avaimella joka johdetaan kortin UIDsta ja "master" avaimesta (ko masteri ei ole sama jolla kortti on formatoitu)
        - Näin jos joku onnistuu häxäämään avaimen jotenkin (tälle fobille ei juuri nyt ole tunnettuja hyökkäyksiä ihmisten budjetissa) niin saa vain oman korttinsa avaimen eikä kaikkia.

Tosin aivan eka revisio alkuperäisen suunnitelman mukaisesti toimii pelkästään kortiin UID:lla <- 2014.09.21 rambo: toimii, tosin jäsenkannasta puuttuu tiedot joten avainkannan generointi on käsipeliä https://app.younited.com/?shareObject=3277f7c0-7334-e6d9-248f-8767118fcfab

Ovissa tms "high security" kohdissa on lukija jonka takana on riittävästi älyä ja tehoa neuvotella noi kryptojutut ja varmistaa että kulkuoikat yms on voimassa (ja ajaa GPIO:n läpi esim solenoidilukkoja). Se että onko tämä raspberrypi vai beagleboardblack (vai jokumuu) on vielä auki.

Nämä älykkäämmät vehkeet saavat kopion kulkuoikeuskannasta alaspäin jäsenrekisteripalvelimelta. ne synkkaavat ylöspäin lokitietoa siitä ketkä ovat kulkeneet ja milloin.

Nämä älykkäämmät vehkeet ottavat myös vastaan UDP(?) broadcasteja tyhmemmiltä vehkeiltä (jos esim työpöytään kuitataan sähköt fobilla, tähän käytetään pelkkää kortin UIDta ja ei tarkistella mitään muuta joka vaatisi krypton laskentaa yms) ja tallentavat tiedot lokiin (joka synkkautuu sitten palvelimelle).

Linux laudan speksit:

- Halpa
- Debian out-of-the-box
- Ethernet out-of-the-box
- RTC olis kiva
- PoE olis superkiva (erityisesti siten että jaksais ajaa releitäkin eikä pelkästään lautaa)

Lokitietokanta:

CouchDB on varmaan aika hyvä, pitää hanskata replikointi siististi ja olla document-store.

Access privileges kanta:

SQLite riittänee enemmän kuin hyvin, liimaksit imuroi esim SCP:llä (public key, no password) tunnuksella jolla on ainoastaan lukuoikeus ko tiedostoon. Jäsenrekisteripalvelin generoi tämän kannan erikseen esim kerran tunnissa.

Jäsenkantaan uudet jutut

- ACL modeli
    - Lyhyt kuvaus, bitin numero
- PersonACL modeli

        - Linkki ACL:n ja personin välille, eli kenelle annettu mitkä oikat
- Card modeli
    - string UID
    - boolean Revoked
        - Kadonneiden tms korttien kuoletus
    - Linkki personiin
        - Yhdellä henkilöllä voi siis olla useampi kortti mutta yleensä vain yksi niistä on jotain muuta kuin revoked

Varsinainen ovien SQLite korttikanta muodostetaan hakemalla ensin revoked kortit toiseen tauluun ja sitten koostamalla henkilöiden korteista ja ACL:stä itse keys-taulun sisältö. ACL:ät ovat siis henkilöön eikä korttiin sidottuja.