Exploring music festivals RFID wristbands

For fun and pr… well just for fun actually.

$ whoami

- Julien Piat (@luminouw)
- Cybersecurity consultant / Pentester @ Adacis

- Discovered the world of RFID and the fun around it during a Pass The Salt free workshop years ago (thx @doegoxx & @herrmann1001)
  - Bought my Proxmark3 literally “on the streets” during the social event : D

- Trying to revive BSides BDX
  - Hit me up if interested :)

$ Context

- Lots of festivals now relying on RFID systems for different operations
  - Access control to the main site
  - Cashless payment for 🍺 (and food, but mostly 🍺)
    - Allows for tracking your spending habits as well …

$ How to explore the tags

- Bring your hardware to the festival
  - Proxmark3 with BTAddon + Termux for on the go operation
  - Have an excuse if asked about it
    - “That’s just my glucose / insulin monitor”
  - Do it at your own risk
    - You can lose it or meet pickpockets

$ How to explore the tags

- Or just do it from home beforehand !

- This year we could have our wristbands delivered at home …
  - Meant to manage the influx of people and access to the festival

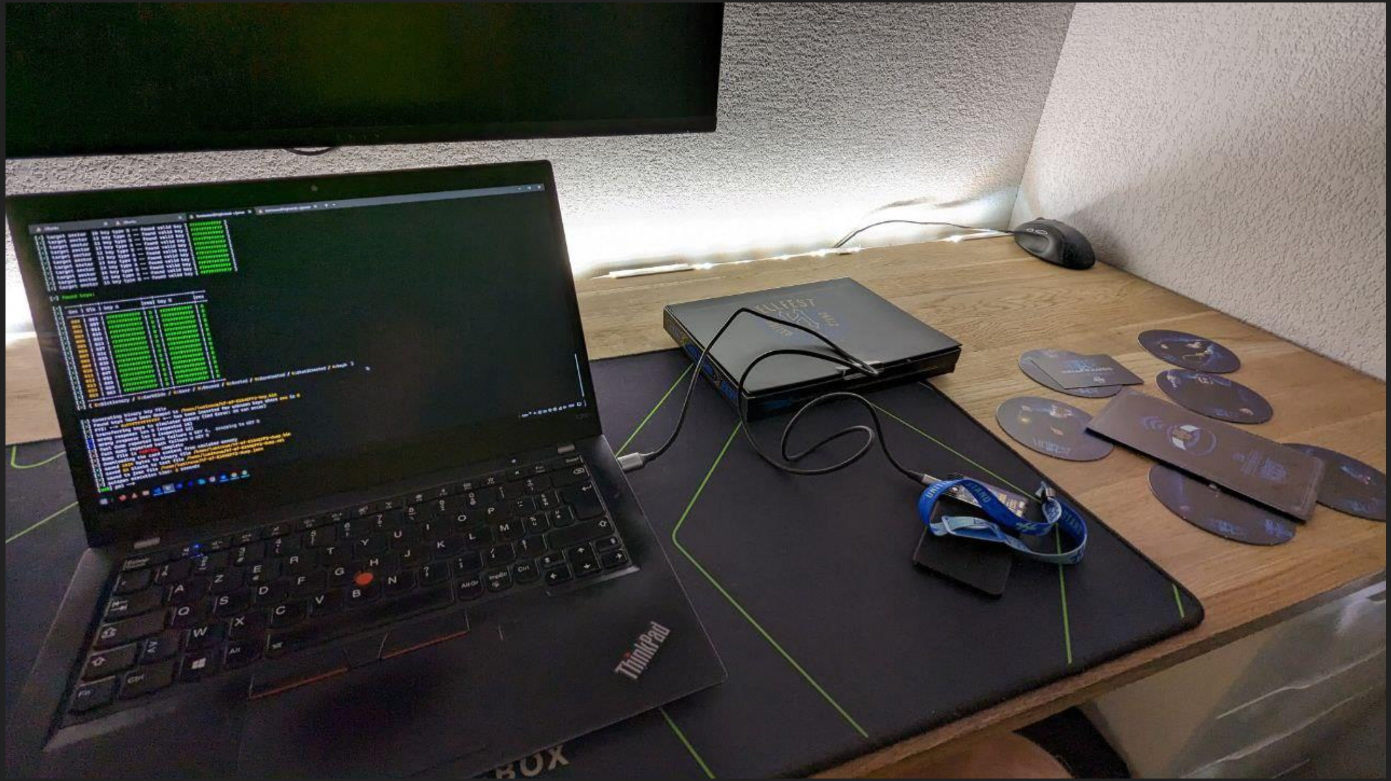
- At home …
  - where I have all the tools to perform analysis …
  - And two weeks before the event …

- Risk assessment meeting be like “we accept the risk 👍”

$ How to explore the tags

"No one will be curious enough to try to dump the tags before the festival."

- Clueless.org



$ Exploring the tag content

- Mifare Classic 1k
  - Fudan variant → Hardened
  - All keys are default
    - Any Android app will dump it gladly
  - Data is all 0
- Well that's one pretty empty stuff …
- The year prior my tag had complex keys and unknown content
  - It must be set when entering the site or during payments

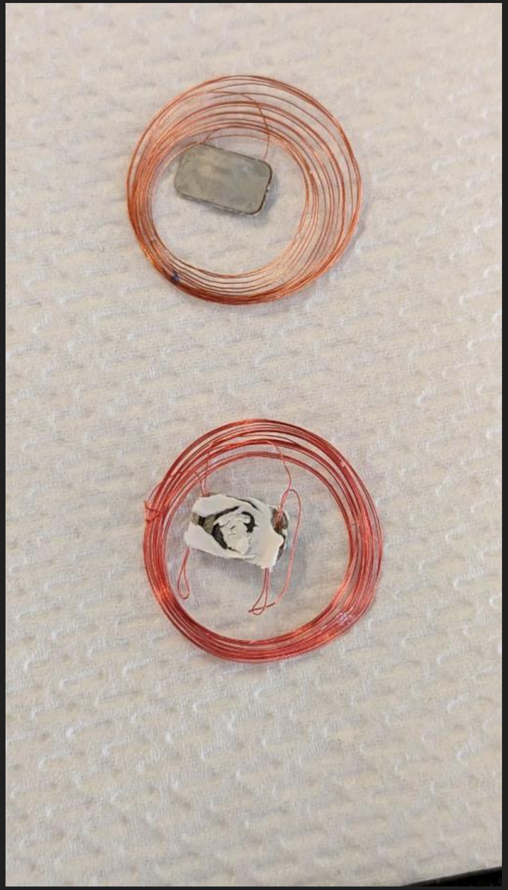
$ The (not so good) idea

- Can’t guess the keys once the tag is written
- No known vuln in the Fudan variant …

- I can sniff the exchange between the reader and the tag when paying for beer and extract the keys
  - Quite suspicious to take out the Proxmark3 when paying in front of a human !

$ The (worst) idea 💡

- Extract a Gen1a chip and antenna from another tag
  - Acetone FTW !
- Wear it next to your real tag, under your wrist …
- Use the clone during the whole festival



$ The (worst) idea 💡

- Gen1a chips have a **backdoor command** that lets you dump the content of the tag without knowing the keys

- Dump after each transaction
- Diff and analyze everything

$ What can go wrong ?

- Readers can detect the backdoor command
- If you get caught, might get banned from the festival …
- Is it worth it ? Meh …

- So I didn’t use the clone … not for now at least.

$ Getting the keys

- I did manage to sniff some keys with the Proxmark3 hidden under a towel next to my wrist \o/

- Diversified algorithm
  - Keys will be different for each tag
  - Different keys for different sectors
  - Probably UID based
    - Algo unknown

$ Tag content

- Able to dump a couple of sectors of my genuine tag
- After some diffing
  - No obvious information (credit, clear text …)
  - Looks like a transaction book
  - Probably signed
  - Probably sync’ed into a backend database

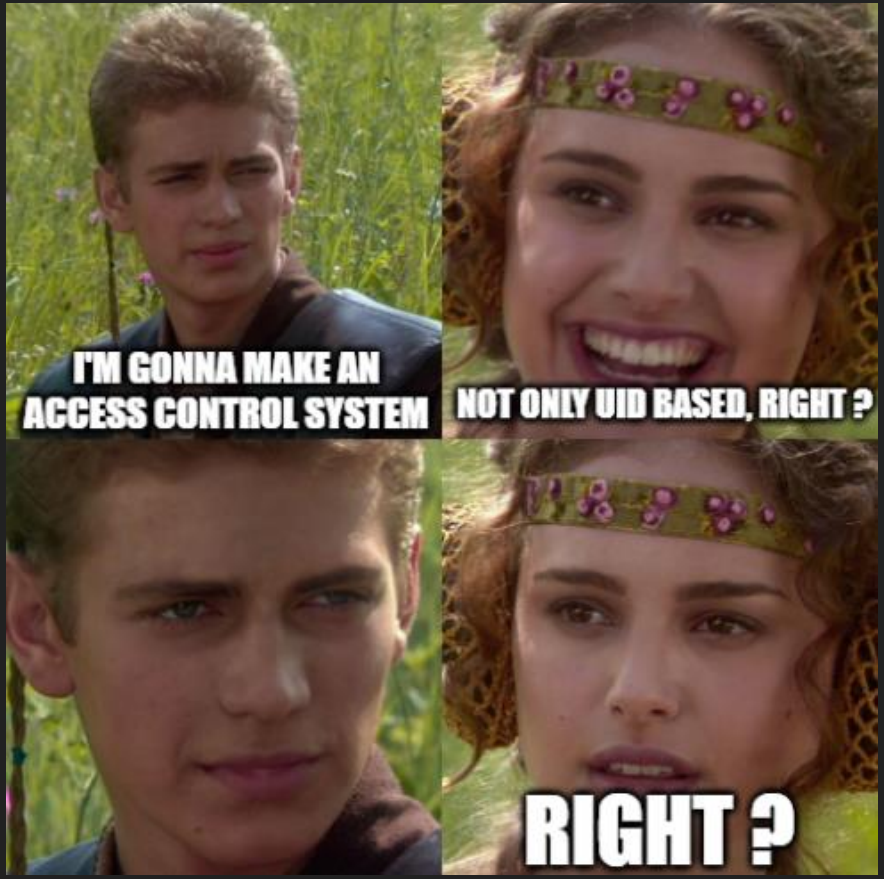
$ What about the clone ?

- I still had my clone that I haven’t used
- It still is untouched at this point (default keys, empty content)
- Different state than the genuine tag

- So it probably won’t work at the gates …

$ What about the clone ?

- Clone worked !
  - None of the keys were changed !
  - Tag still empty !
  - Backdoor not checked !
- … only UID based ?!
- Also no passback protection so yeah, that's something.
- Readers are online and show your name on a screen (UID ←→ ticket holder in a DB)


I'M GONNA MAKE AN ACCESS CONTROL SYSTEM
NOT ONLY UID BASED, RIGHT ?
RIGHT ?

Thank you 🤘

Keep calm and rock on :]