

HACK THE WORLD & GALAXY WITH OSINT

OWASP LONDON

CHRIS KUBECKA, CEO HYPASEC

19 SEPTEMBER 2019

WHO IS THIS CHICA?

- Cyber Warfare
- Headed Aramco Overseas Operations, Information Pro & Intelligence
- U.S. Air Force Space Comm Military Aviator C-5 Loadm



"Join The Space Force" they said

DO YOU WANT HACKERS



**BECAUSE THATS
HOW YOU GET HACKERS**

SECURITY & PRIVACY CHALLENGES

Large number
of access points

Renewable
energy systems
entry points

Electricity theft

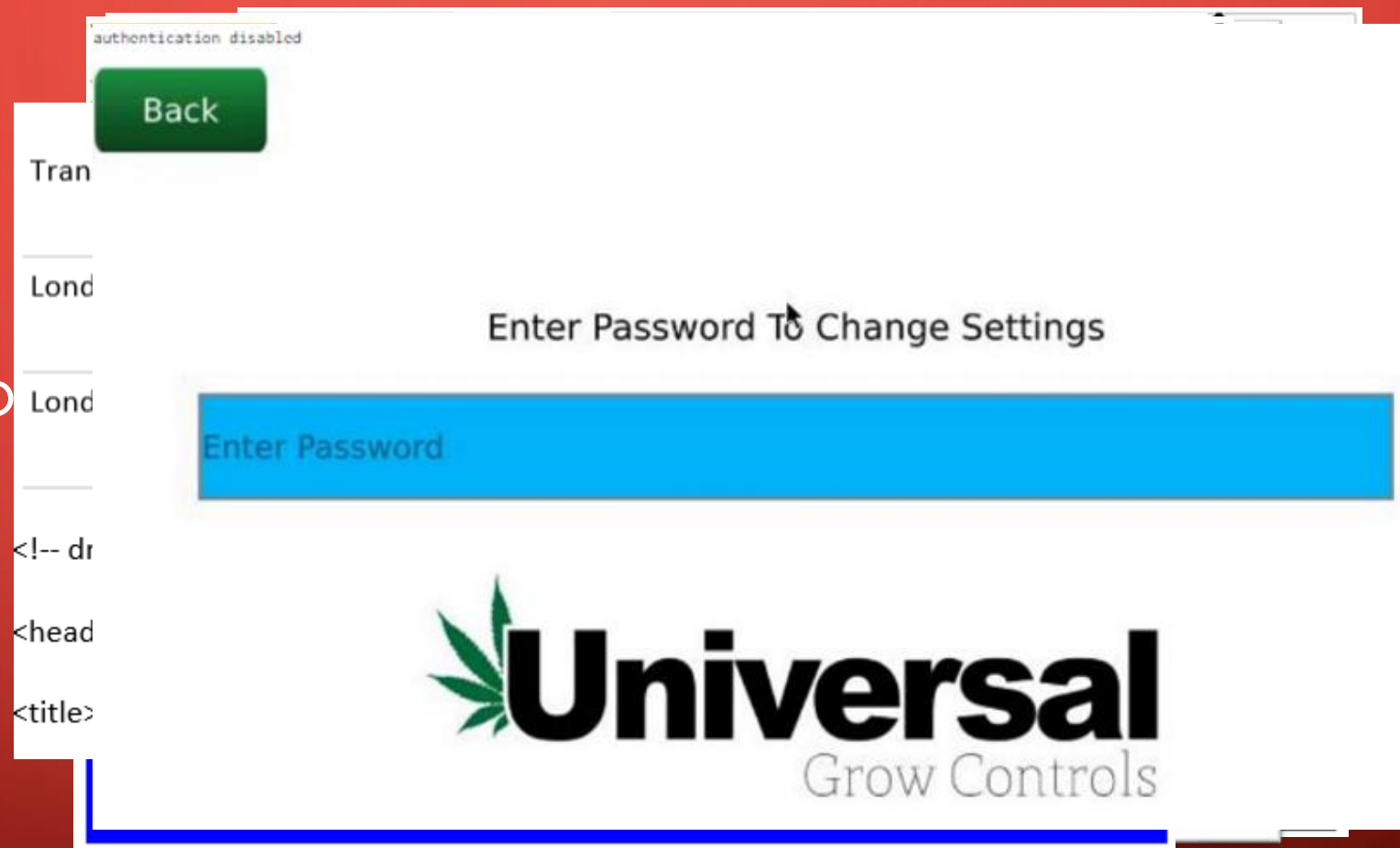
Most equipment
privately owned

Lacking
standisation

Security an
afterthought

CRITICAL INFRASTRUCTURE

- Power plants
- Water systems
- Agriculture
- Hydroelectric D
- Railway
- Logistics
- Weed



SOLAR & WIND

- Crucial for the P...
- Load manag...
- Climate ch...
- Many vendors
- Not much security testing
- Bonus

IPv4 Hosts

Page: 1/3,519 Res

 77.243.63.



 NETIC-AS

 Ubuntu

 myWindTu

 80.http.ge

Tag:

651 scada
 651 solar panel
 622 modbus
 358 http
 248 ftp
 49 ssh
 29 building control
 29 fox
 25 https
 17 NPM
 13 NPM6
 10 JACE
 10 JACE-7
 9 embedded
 8 telnet
 4 NPM2
 3 dns
 2 database
 2 mssql
 1 bacnet

 Less

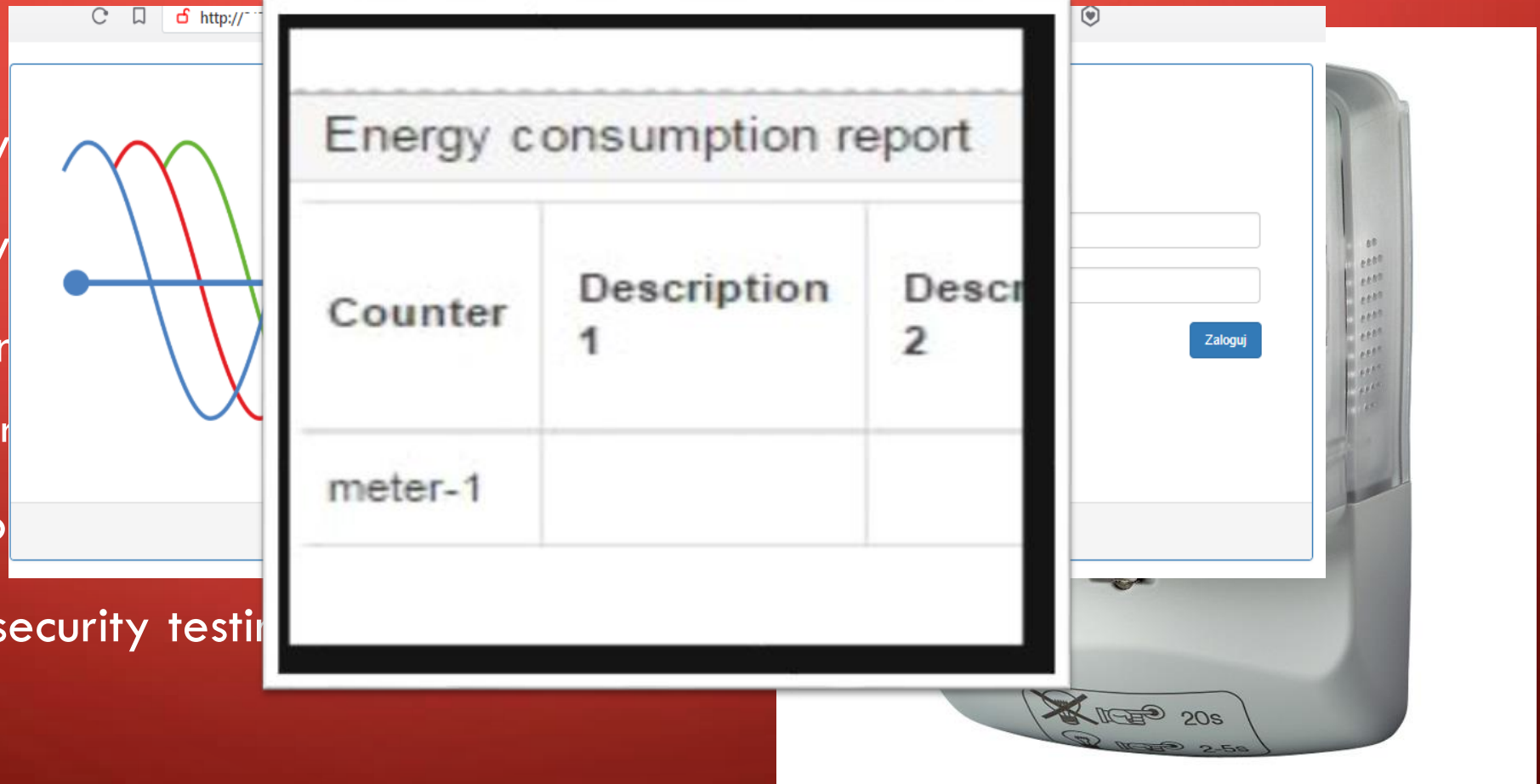
denmark, Denmark

1"

rwindturbine.com
 myWindTurbine

SMART ELECTRIC METERS

- Mandatory
- Mandatory
- Privacy concerns
 - Can be read remotely
- Security concerns
- No cyber security testing



OPEN AUTOMATED DEMAND RESPONSE

- North America
- Interoperability
- Pricing
- Demand
- Controls all components
- Zero security

 Chrome TLS

Cip

Tag:

58 https

52 http

27 ssh

3 ftp

1 DSL/cable modem

1 database

1 embedded

1 mysql

1 postgres

1 smtp

IA (0x0035)

unknown authority

A Brief HISTORY of SELF-REGULATION

```

220- #####
220- #
220- ##### #
220- ## ## # #
220- ## ## # #
220- ##### #
220- ## ## #
220- ## ## #
220- ## ## FWAG #
220- #
220- -----#
220- #
220- FTP Flughafen Wien AG #
220- #
220- datahub.viennaairport.com #
220- #
220- This is a private system operated for and by #
220- Vienna International Airport. Authorization #
220- from Vienna International Airport is required #
220- to use this system. #
220- #
220- Telephone No.: +43-1-7007-25353 #
220- #
220- #####

```

VIATION

You are lo

Al

Unauthoriz

Network Devices

logged

lines.com

port

FINANCIAL SECTOR

AIRLINE INDUSTRY

US AIRCRAFT MANUFACTURER

- No current coordinated disclosure



CISA
CYBER+INFRASTRUCTURE

```
reserved.</p>
<br/>
<!-- #no idea what this was trying to print but only says
</center></div>
NULL -->
<!-- ### END FOOTER ### -->
<center>
<font color="gray" size="-2">
<p>
</p></center>
</font>
<br>
</center>
</font>
<p><font color="gray" size="-2"></font></p></center></div>
<!-- Adobe Analytics Code -->
<script type="text/javascript">
if (typeof _satellite !== "undefined") {
_satellite.pageBottom();
} else {
```

Then the other side to see what for instance general coding practices look from the outside. This is from the [redacted] login website

04/08/19, 17:25 ✓

LOL - you probably shouldn't extrapolate from the web site to flight control code.



Ubiquiti Networks Device
IP: 95.130.58.101
MAC: 04:18:d6:96:52:1c
Alternate IP: 192.168.1.20
Alternate MAC: 04:18:d6:97:52:1c
Hostname: **HACKED**-ROUTER-HELP-SOS-HAD-DUPE-PASSWORD
Product: LM5
Version: XW.ar934x.v6.0.3-licensed.30600.170329.1947

For all details, see [Nessus Scan Results](#)

Page: 1/10,248 Results: 130,181 Time: 17:41:18

Marine HMI ECDIS Panel PC

I330 EAC

Sensor

Revolutionary Guard vessels. Photograph: AP

stem

d IIOT

SPACE ASSET CHALLENGES

- Legacy equipment
- Interoperability
- IOT
- Lack of Encryption
- Nation-state attacks
- Solar weather
- Radiation flipping
- Surveillance
- Manipulation
- Debris
- Loss of visibility
- Low cost uncontrolled launches

Threats to satellites and who are the assailants?

- MITM attacks with lasers
- Physical takeover of satellites
- Physical attacks (including natural solar flares, meteorites etc)
- Crack the encryption of command line to kill off satellites or read all comms.
- Side channel attacks?
- Nation states/hacktivists etc
- Multinational corporations
- Jeff Bezos
- Elon Musk
- Mark Zuckerberg and other aliens

DISCOVERING IOT SPACE ASSETS

- Tool used Censys.io
- Free
- Vulnerabilities
 - DNP3 Protocol
 - Modbus Protocol
- Working to expand Censys

148.78.230.138 (misc-148-78-230-138.pool.starband.net)

- [Summary](#)
- [WHOIS](#)
- [Raw Data](#)

Basic Information

	SPACENET-GTH — Spacenet, Inc. (US)	Network
	148.78.230.0/24 via AS7922 , AS7725 , AS16811	Routing
	20000/DNP3 , 502/MODBUS	Protocols

20000/DNP3

Details

Device Information

	True	Support
	BWQFCwAAQC68A==	Raw Response

502/MODBUS

Details

MEI Device ID

http://[redacted].adsl.highway.telekom[redacted]

NO GIMMICKS.
REAL SMART HOMES.



Loxone Web Interface

Username

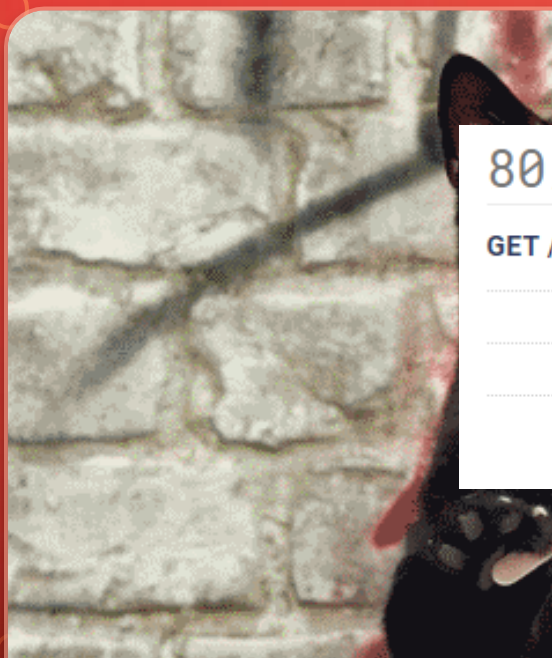
Password

Connect

SE?

iele
R BESSER

iele & Cie. KG



QUESTIONS & THANK YOU

- Thanks to @Beauwoods @Orbit_RRI & @UnivOxford, FAIR Space Hub, Royal Holloway, EU Commission
 - Darknet Diaries Shamoon episode 30
 - https://en.m.wikipedia.org/wiki/Chris_Kubecka
 - *When the internet gives you remotely exploitable systems, take them. They're like free candy, right?*
- Chris Kubecka

