



INSIGHTS INTO HACK ATTACKS ON SMART GRID & THE USA FRAMEWORK

AUSTRIAN EU PRESIDENCY CONFERENCE CYBER SECURITY IN THE
ENERGY SECTOR

CHRIS KUBECKA, CEO HYPASEC

11 OCTOBER 2018

BIOGRAPHY

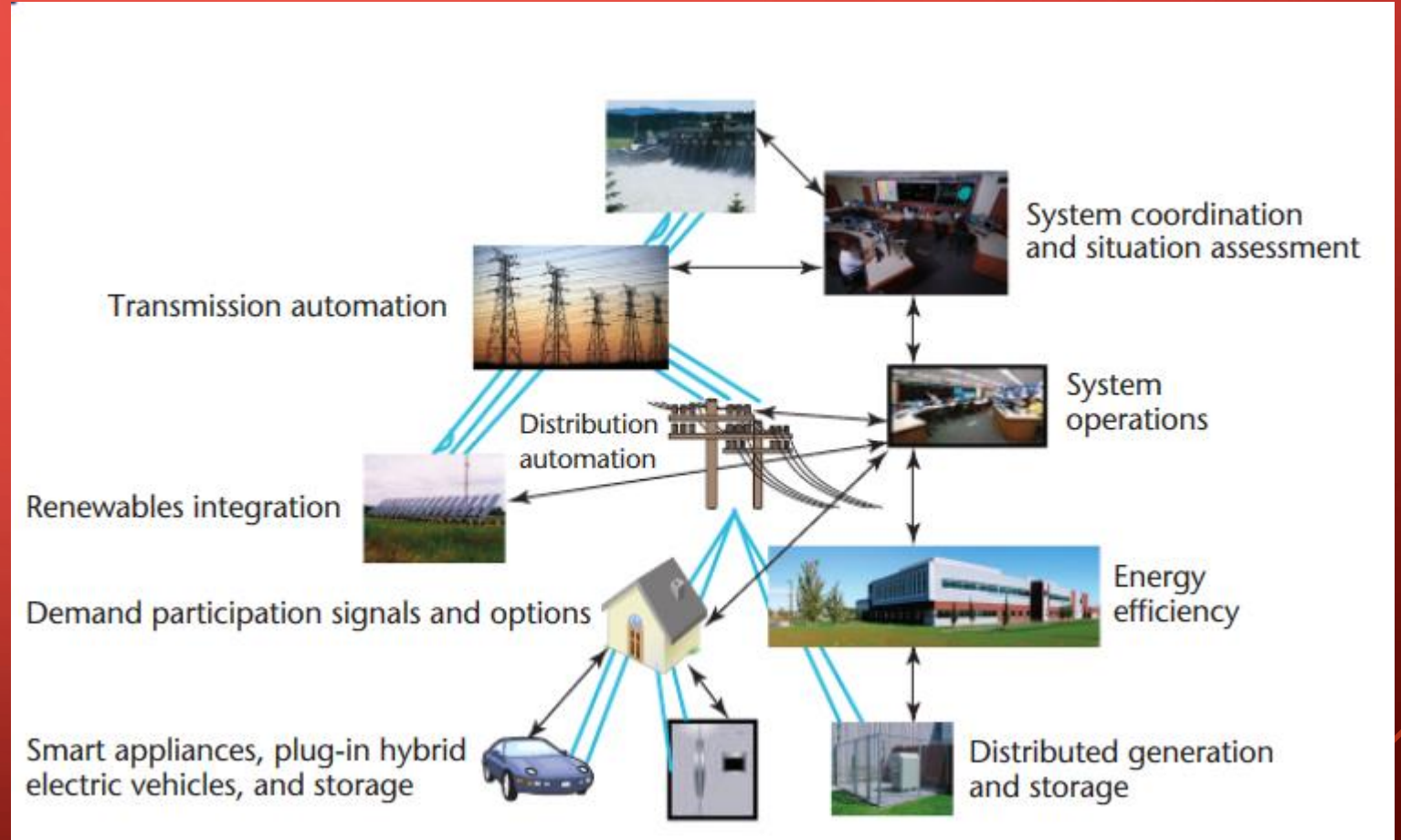
- Cyber warfare incident management and advisement
- Critical infrastructure security expert: Oil & Gas, Water, Electric & Nuclear
- Author, presenter at Black Hat, Security BSides, ICS/SCADA Nuclear Cyber Security
- Previous headed Aramco Overseas Security Operations, Information Protection & Intelligence
- Previous U.S Air Force Space Command
- Previous script kiddie hacking the US Government

US SMART GRID FRAMEWORK INTRODUCTION

- Bi-directional
- Resilient
- Near real-time data collection
- Encryption
- Interoperable
- Load Shedding
- Increased efficiency

SMART GRID COMPONENTS & TECHNOLOGIES

- On-demand
- Renewables
- Electric transport
- Smart appliances
- Auto Load-balancing
- Sub stations
- Smart homes
- Smart buildings
- Smart cities



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

LOGIC CONTROLLERS PLC

- Programmable
- Provides the logic for automation
- High value target
- Stuxnet
- Weak Link

```
80.http.get.body: Portal/Portal.mwsl
```

```
80.http.get.title: SIMATIC 300
```

```
"80": {
  "http": {
    "get": {
      "body": "<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Tr
\n  <title>\r\n    SIMATIC 300(1)\r\n    </title>\r\n    <MET
<body>\r\n      <a href=\"/_INTERNAL_Portal/Portal.mwsl?M
```



SOLAR & WIND

- Crucial for the Paris Acco
- Load management
- Climate change
- Many vendors
- Not much security testing

IPv4 Hosts


Page: 1/3,519 Results: 87,974 Time: 160ms

 [77.243.63.16](#)

 NETIC-AS (42697)  Aalborg, North Denmark, Denmark


 Ubuntu  443/https, 80/http

 myWindTurbine 1.0.13965  www.mywindturbine.com

 80.http.get.body: a wind turbine . myWindTurbine

Tag:

ar panel"

1320)  Germany

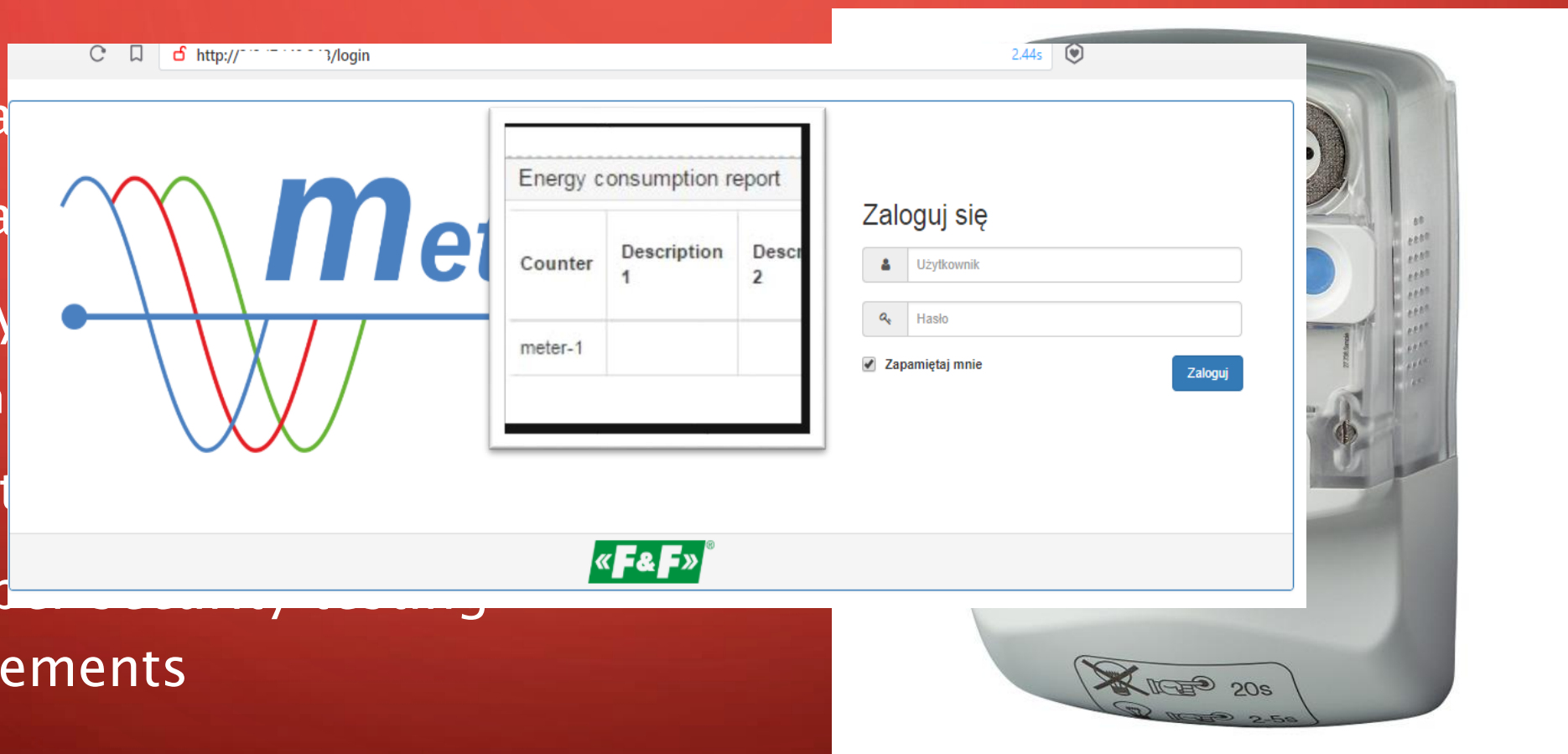
Panel

4 NPM2
3 dns
2 database
2 mssql
1 bacnet

 Less

SMART ELECTRIC METERS

- Mandat
- Mandat
- Privacy
 - Can
- Security
- No cyber security requirements



OPEN AUTOMATED DEMAND RESPONSE

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

Chrome TLS Handshake

Version TLSv1.0

Cipher Suite TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Trusted False : x509: certificate signed by unknown authority

52 [REDACTED]

MICROSOFT-CORP-MSN-
443/https
hydroquebecvtn.openadi
443.https.tls.certificate.p

Tag:

58 https
52 http
27 ssh
3 ftp
1 DSL/cable modem
1 database
1 embedded
1 mysql
1 postgres
1 smtp

(5) Québec, Quebec, Canada


R Alliance

ilding Solutions SGS,



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

NO GIMMICKS.
REAL SMART HOMES.



Loxone Web Interface

Username

Password

Connect

A



iele
R BESSER

.....
iele & Cie. KG



13 days later

**Your strategic supply is
gone!**

GAMEOVER

CONCLUSION

- Proactivity
- Security testing
- Don't assume its okay
- Connect after assessment
- Prepare for attack

QUESTIONS & THANK YOU

- Chris@hypasec.com
- [@SecEvangelism](#)
- Hacking the World with OSINT & Censys – Released next week
- Down the Rabbit Hole an OSINT Journey, Author

*When the internet gives you remotely exploitable systems, take them.
They're like free samples, right?*

– Chris Kubecka