How an intern hacked the power grid

The Horus Scenario

Who am I?

- Willem Westerhof
- System & Network engineering
- White-hat @ ITsec/Qbit
- Pentesting/Vulnerability assessments
  - Password cracking
  - Consultancy/advisor
  - Workshops and training
  - Public speaking

Today’s Content

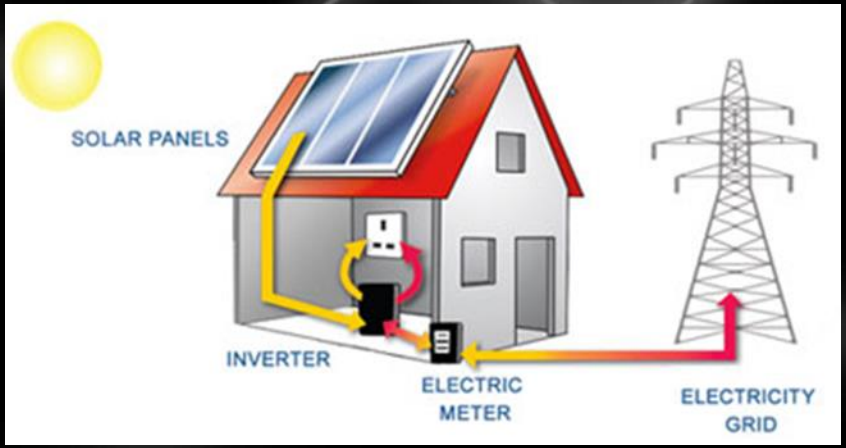
- Context
- The concept
- Theoretical approach
- Practical approach
- Analysis
- Conclusions
- Ongoing discussion
- Questions

Context

- When?
- Why?
- Horus scenario?
- Hypothesis
  - “Photo Voltaic (PV) installations connected to the power grid and their accessories contain security vulnerabilities which allow hackers to influence the power grid in such a way that power outages can occur.”

The concept

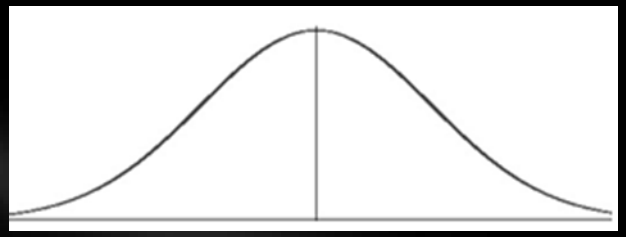
- PV installations
- Constant balance
- Scale is key
- Connected



Theoretical approach

TA: Statistics

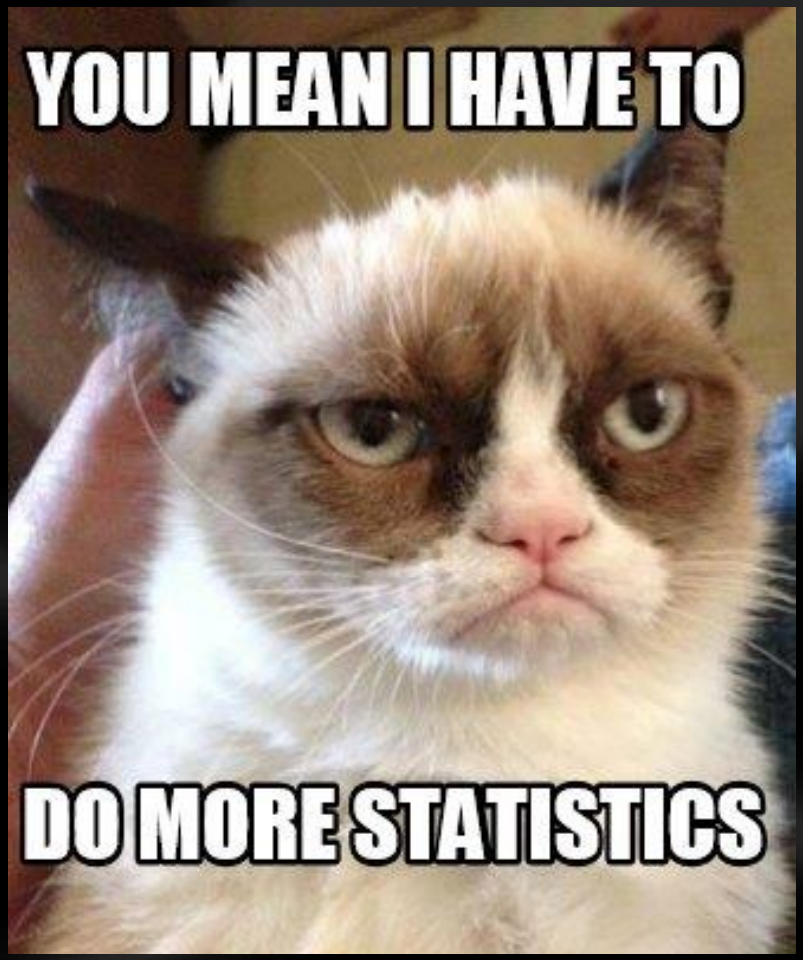
- Statistical approach
  - CBS
  - Distribution of sunlight
- Assumptions & formulas
  - + / - 4.3% in Dutch power grid
  - Equivalent to …



TA: Statistics

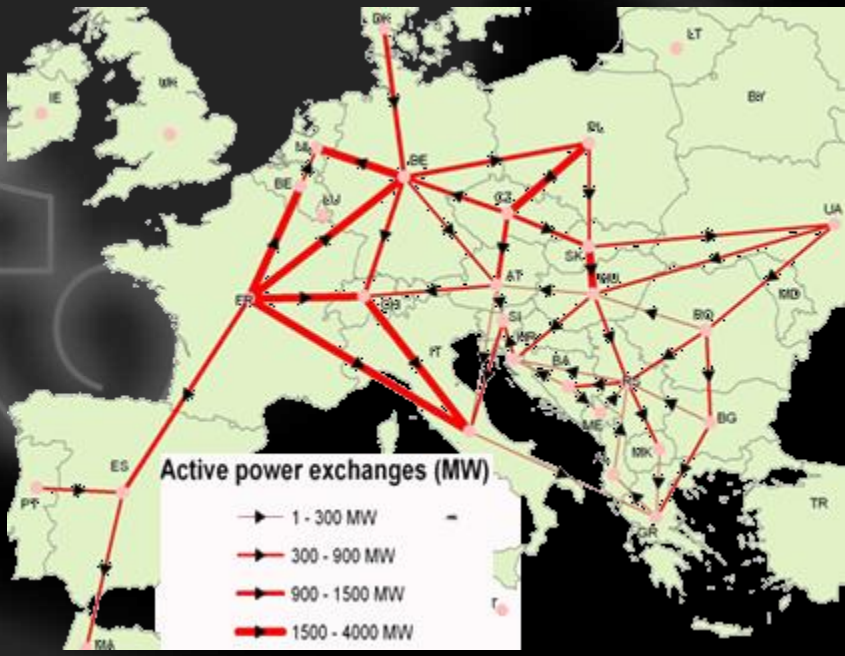
- Power demand of
  - 1.33 Mln households
  - Every household in
    - Groningen
    - Amsterdam
    - Den Haag
    - Utrecht
    - Rotterdam
    - Eindhoven
    - Tilburg

And some more…

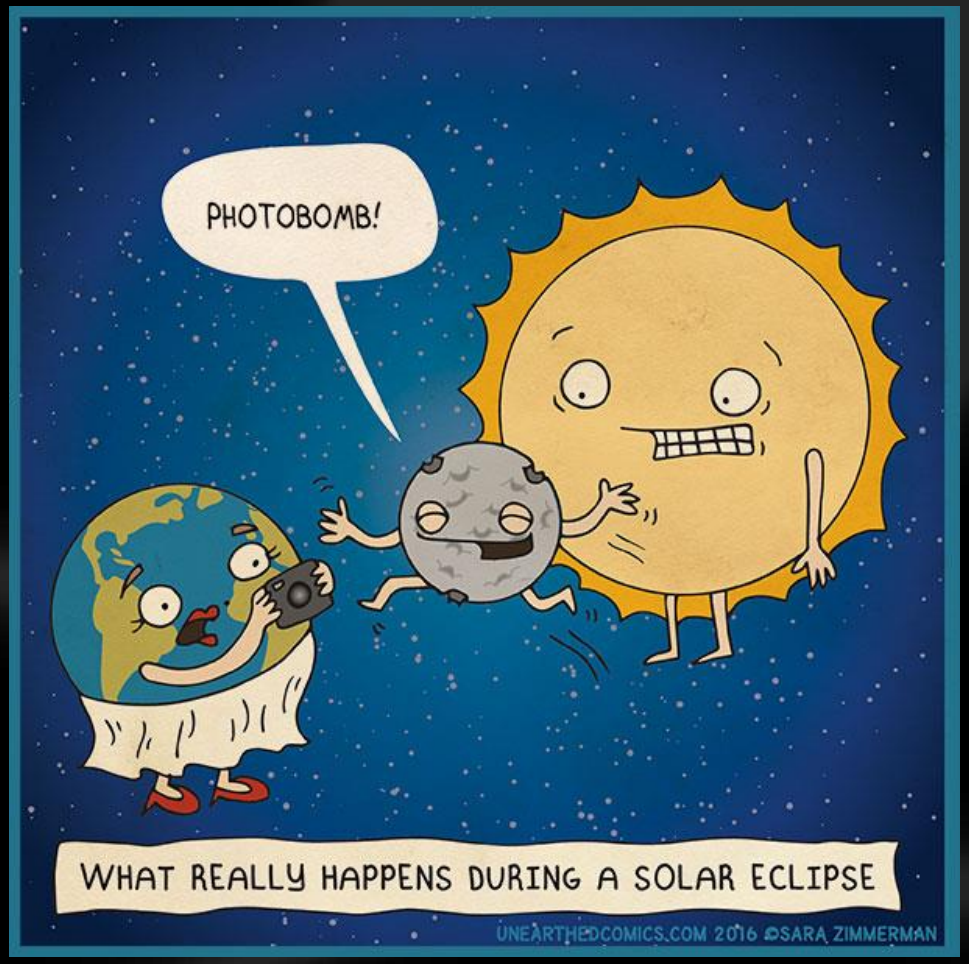


TA: Statistics

- German power grid
  - + / - 35% up to 50%
  - Massive impact
- Europe
  - Intertwined
  - Affects other countries
  - Most PV power
- Power grid regulators
  - Not expected to withstand this attack

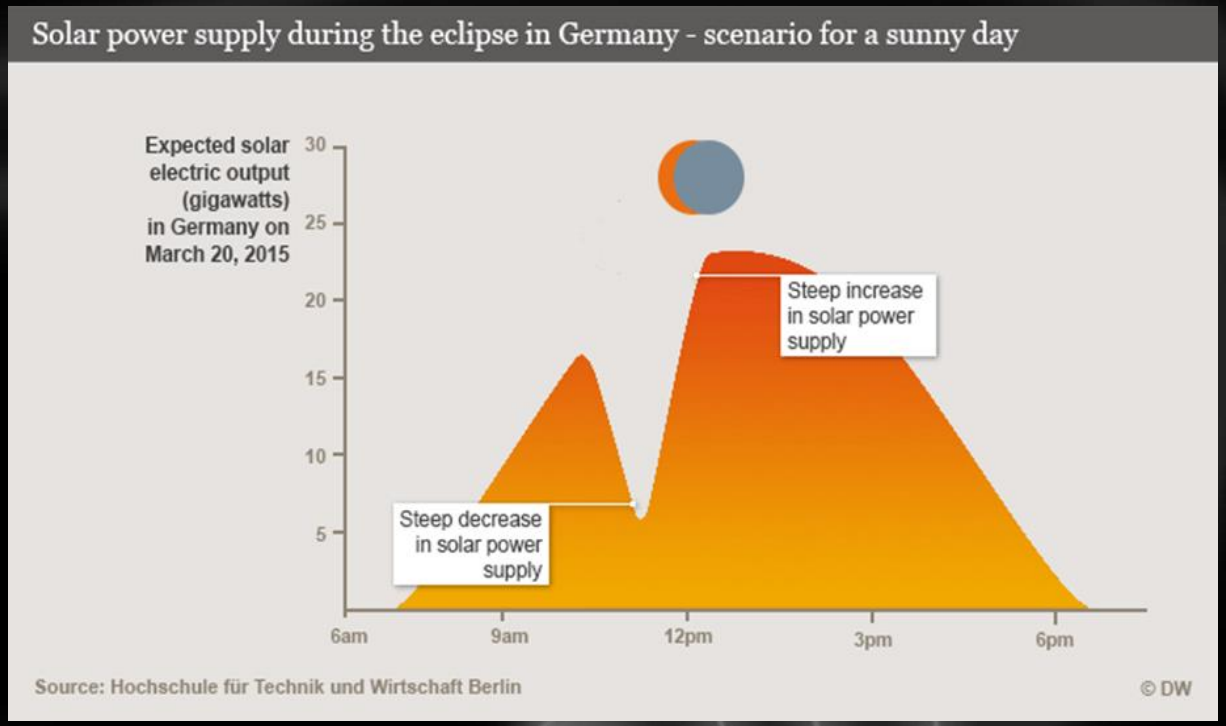


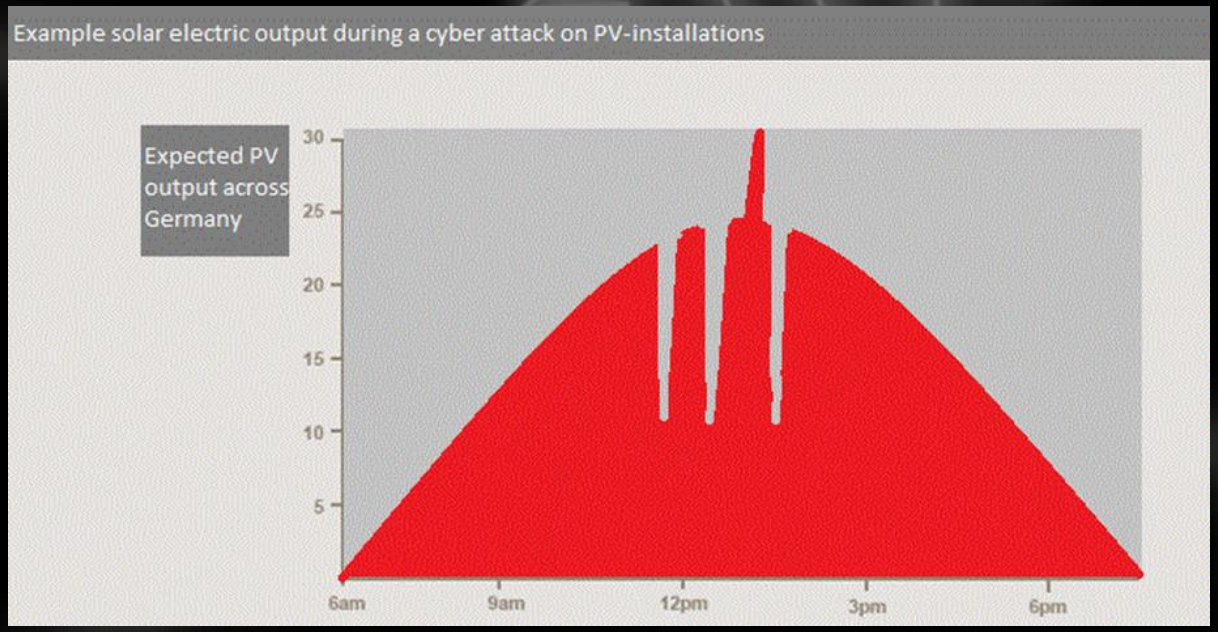
Another way


PHOTOBOMB!
WHAT REALLY HAPPENS DURING A SOLAR ECLIPSE
UNEARTHEDCOMICS.COM 2016 ©SARA ZIMMERMAN

TA: Comparison

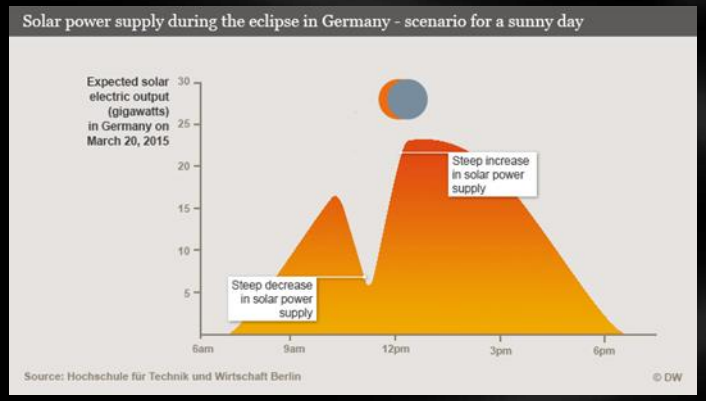
- Solar eclipse 2015
  - Fully prepared for
  - 2-3 hours
  - Expected pattern
  - All PV installations affected
  - Happened in the morning
- Cyber attack
  - Not prepared for
  - + / - a minute
  - Random pattern
  - Expected 50% of PV installations affected
  - Happens during peek suntime

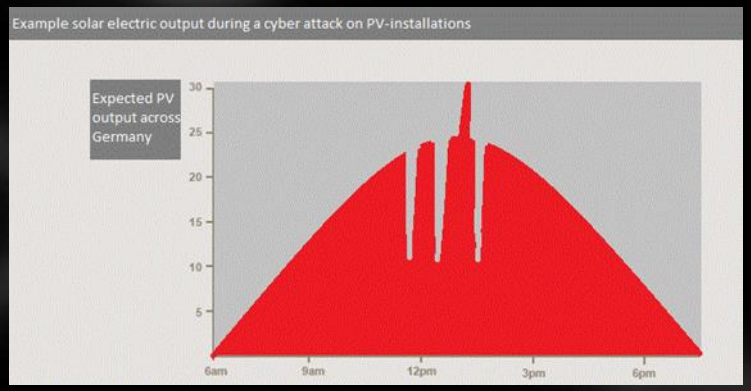

Solar power supply during the eclipse in Germany - scenario for a sunny day
Expected solar electric output (gigawatts) in Germany on March 20, 2015
30
25
20
15
10
5
Steep increase in solar power supply
Steep decrease in solar power supply
6am
9am
12pm
3pm
6pm
Source: Hochschule für Technik und Wirtschaft Berlin
© DW


Example solar electric output during a cyber attack on PV-installations
Expected PV output across Germany
30
25
20
15
10
5
6am
9am
12pm
3pm
6pm

TA: Comparison

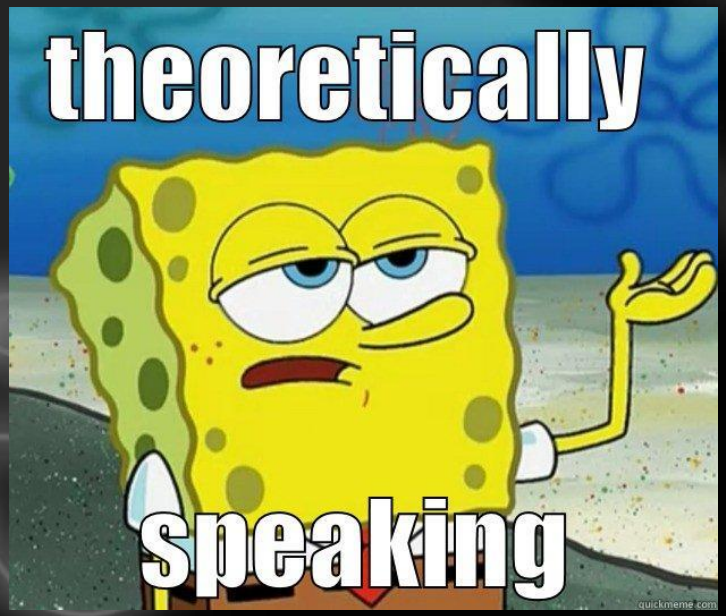
- Conclusion
  - Cyber attack is worse
  - Power grids with a lot of PV power affected heavily
  - Intertwined power grids



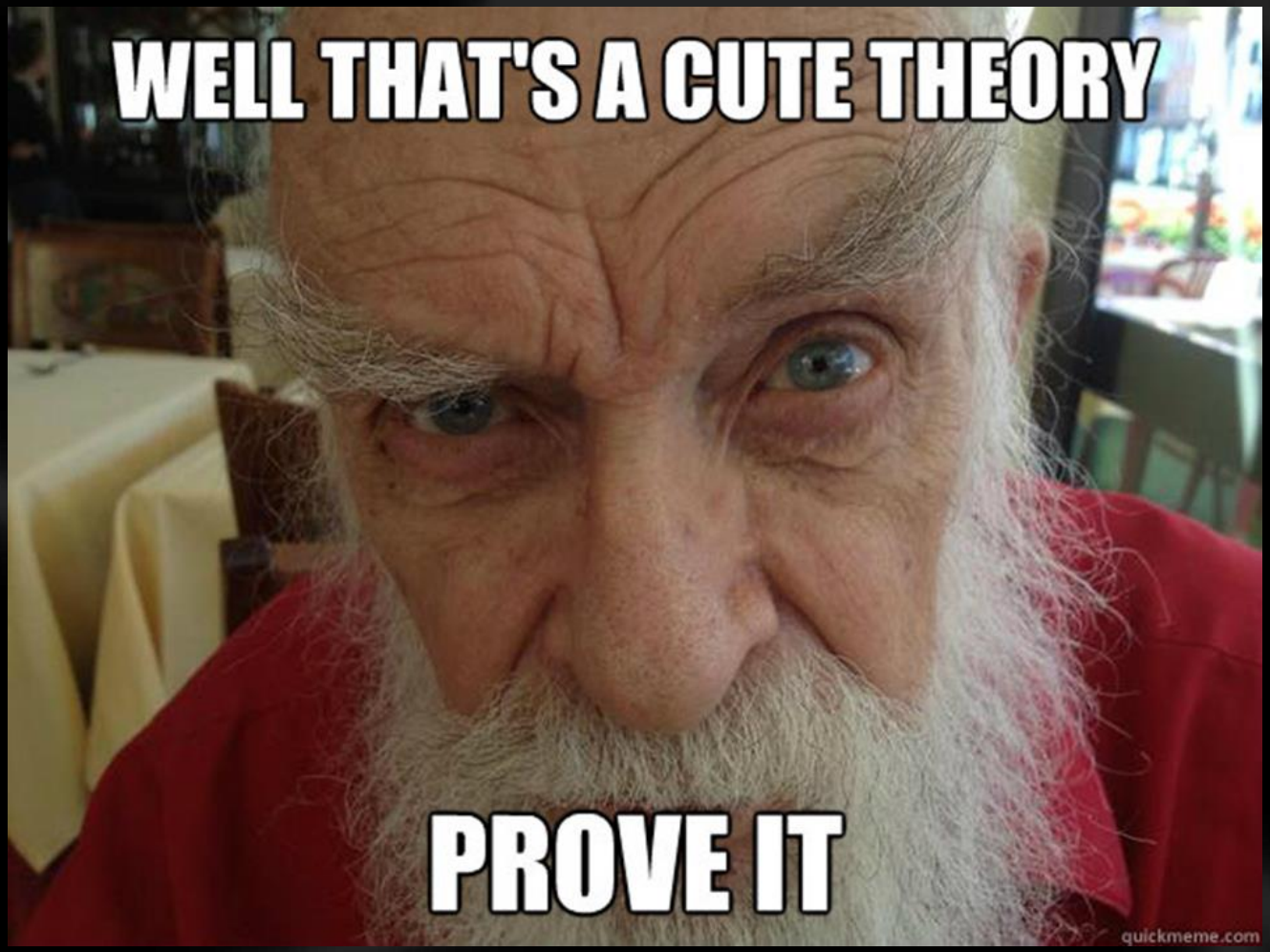


TA: conclusion

- Statistically
  - Serious impact
  - Expected power failures
- Comparison
  - Cyber attack is worse
  - Expect large scale power failures
- Theoretically possible
  - Ticking clock…



Practical approach



Practical approach

- Open source info
  - Test setup selection
  - Laws & certifications
  - Technical documents
- Normal behaviour
  - Open source info
  - Observations in the field
- Black box testing
  - Exploratory testing

PA: Test setup selection

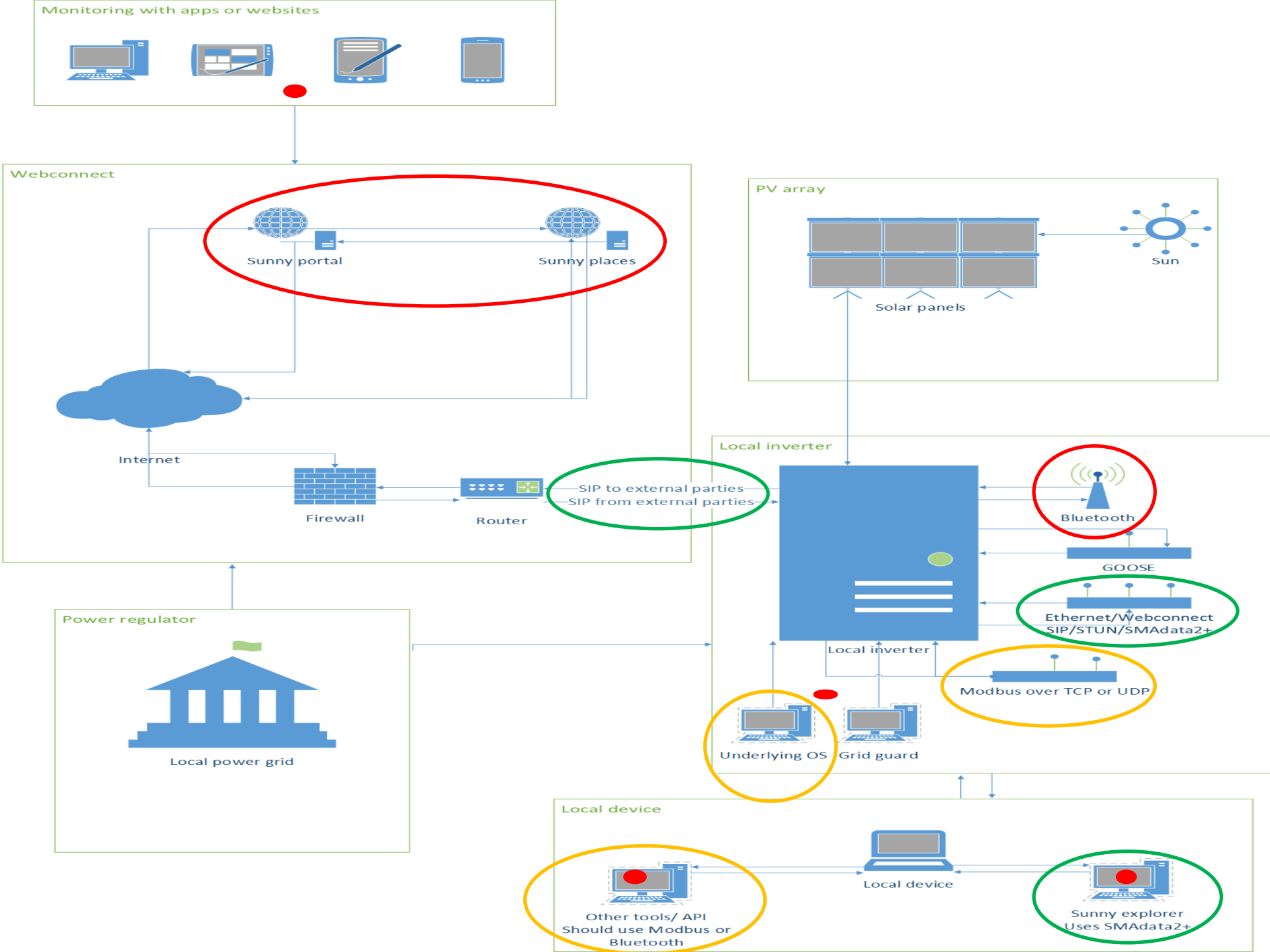
- Criteria
- Selected test setup
  - Any PV module
  - An SMA inverter
- Real life test setup
  - 161 PV modules
  - 2 different SMA inverters
  - € 75.000
- Safety

PA: Cybersecurity measures

- Standards for PV installations
  - IEC 62443, IEC 62351, ISO/IEC 27000
  - Not obliged
  - Expected cybersecurity measures
- Test setup specific
  - Dutch/German cybersecurity law
  - Interview with SMA spokesperson
  - Technical documentation

PA: Normal behaviour

- SIP
- SMAdata2+
- Modbus
- Operating System
  - DNS
  - ICMP
  - ARP
  - IGMPv2

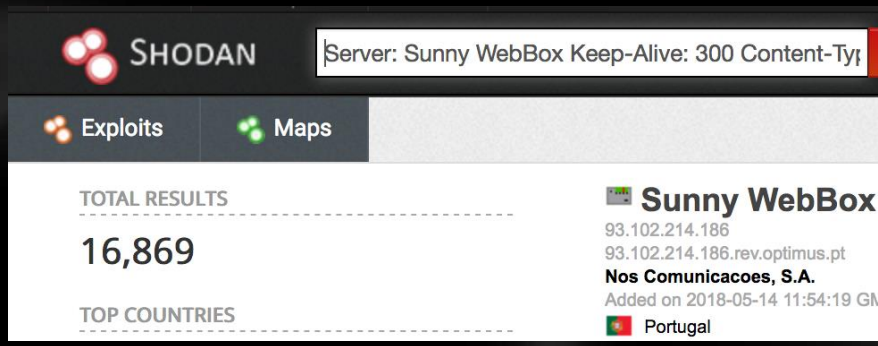

Monitoring with apps or websites
Webconnect
Sunny portal
Sunny places
Internet
Firewall
Router
SIP to external parties
SIP from external parties
PV array
Sun
Solar panels
Local inverter
Bluetooth
GOOSE
Ethernet/Webconnect
SIP/STUN/SMAdata2+
Local inverter
Modbus over TCP or UDP
Underlying OS
Grid guard
Power regulator
Local power grid
Local device
Local device
Other tools/ API
Should use Modbus or
Bluetooth
Sunny explorer
Uses SMAdata2+

PA: Field tests intro

- Too much to discuss right now
  - Old, but relevant findings
  - Finding information
  - Exploit via passwords
  - Exploit via firmware
- No full technical details today
  - Still unknown if fixed
    - Probably not… ☹

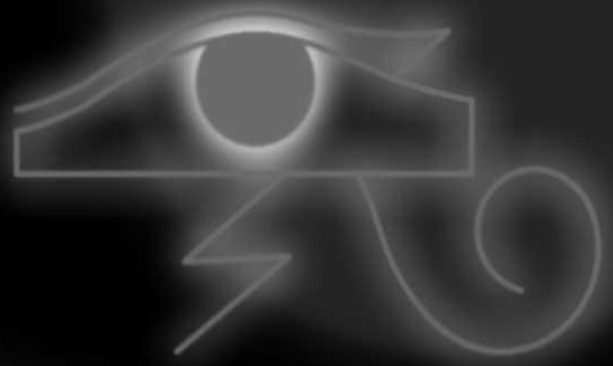
PA: Old, but relevant

- CVE-2015-3964
  - *"SMA Solar Sunny WebBox has hardcoded passwords"*
- Shodan initial search: +/- 10.000 webboxes
- 2 weeks after "live": +/- 4000 webboxes ☺
- Yesterday's search: +/- 17.000 webboxes ☹

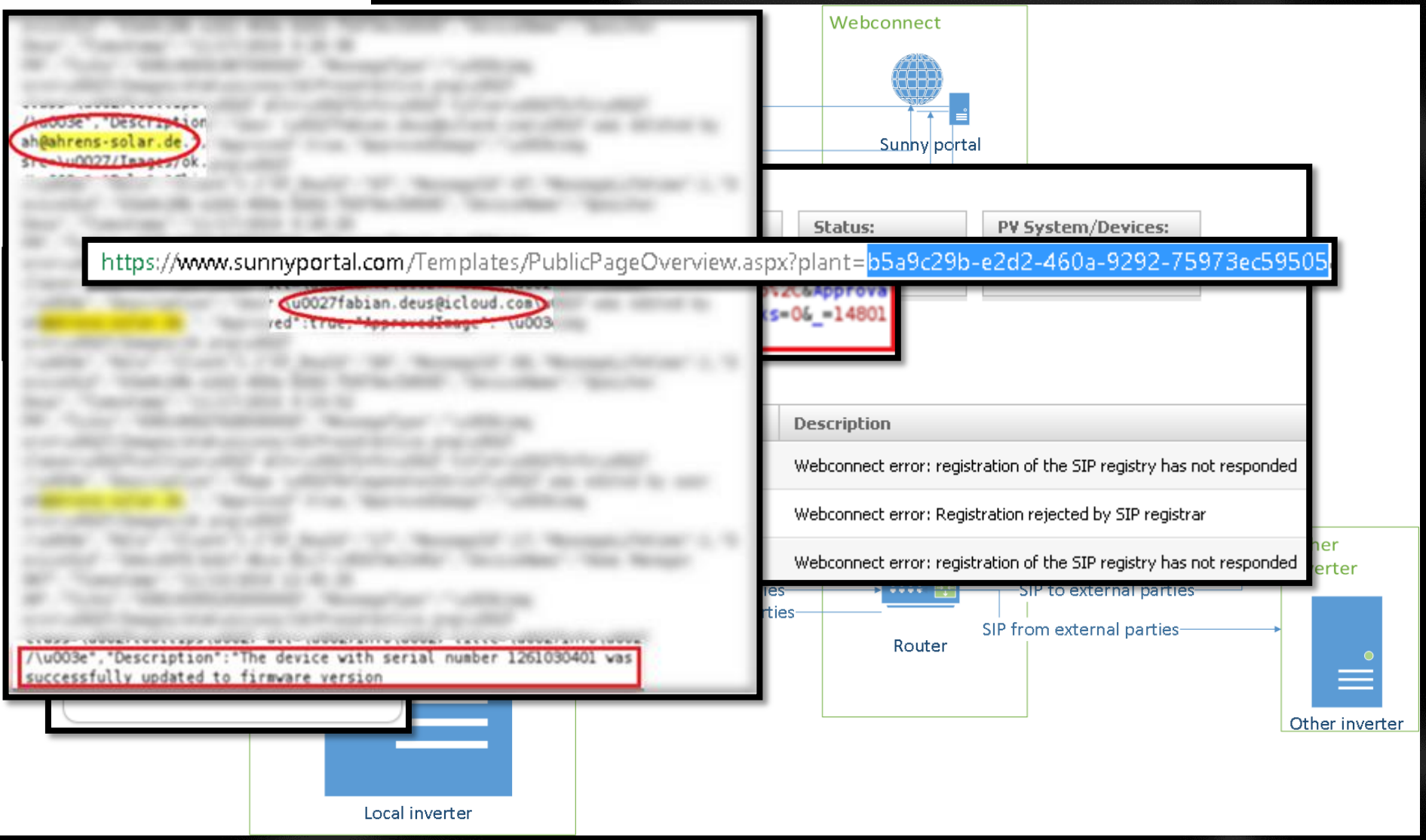


Finding information

- Full technical disclosure on inverter eventlog



PA: Inverter event log



Exploit via passwords

- Passwords
  - Policy
  - Sniffing
  - Brute forcing/targeted guessing
  - CSRF
  - Master passwords
    - User enumeration shows multiple hidden users
- Exploit
  - Change settings with granted rights

Exploit via firmware

- No user credentials required
- Uses one of the “nonexistent” secret passwords
- Flashes firmware succesfully
  - Pass the checks to win ☺

Simar testing R2 - Sunny Explorer

File Options Tools Help

SUNNY EXPLORER

Simar testing R2
- Sunny Explorer
- SN: 2110559838
- SN: 1900739342

User 12:01:32

Device update

SUNNY EXPLORER

Help

Update Process

The following update file has been loaded to your system:

C:\...oads\FW2.83_STP_15_20_25000TL-30\Update\STPxx000TL_30_V2.83.03.R.up2

To close the dialog, select the [OK] button.

OK

And many more

- Other discovered vulnerabilities
- Other expected vulnerabilities
  - Untested due to constraints
- Several untested attack scenarios

PA: conclusion

- SMA devices contains vulnerabilities
  - Allow control of stopping and starting power output with and without access rights.

Analysis

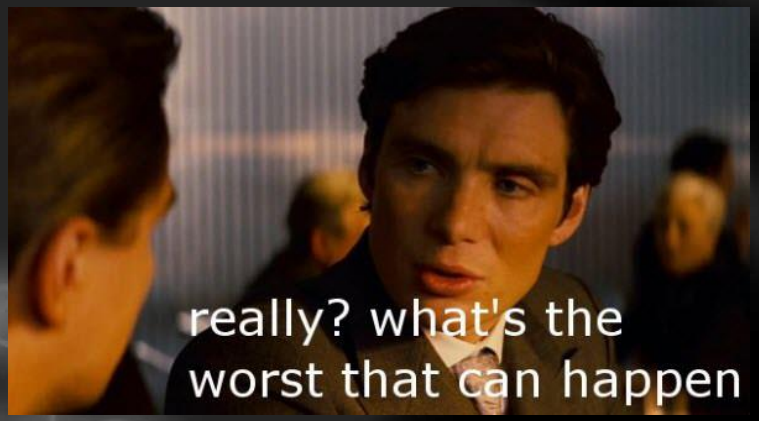
- Generalisation
- Confirmation
  - *"Possible 100.000 solar meters vulnerable for security issue"*
  - *"Citizens Emmen victim of databreach due to Solar panels"*
  - *"Shodan shows 17.000+ SMA webboxes"*
  - *Tweakers.net comments…. & PM's*
  - *No news of fixes…* ☹
- Theoretical possibility
- Practical possibility

- Indicators show it is possible
- What to expect?

Best case scenario

- Not enough devices
- Power on
- Vendors start patching a.s.a.p.

Worst case scenario



- Enough devices
- Power outage
  - Import / export
  - Other power sources
  - Recovery is very hard
- Financial impact (Blackout calculator)
  - The Netherlands: € 156.150.000
  - Germany: € 836.890.000
  - Europe: € 4.435.390.000
  - Hundreds of millions, if not billions, in damage
- Indirect effects

Conclusion

- Assumptions
  - SMA brand is representative
  - Technically skilled / resourceful attacker
- Hypothesis confirmed

- Recommendations
  - PV companies
  - Government officials
  - Consumers
  - Further research

- No bugbounty ☹

Discussion

- What was being discussed:
  - Can an attacker actually compromise that many devices?
  - Political agenda…
- What should be discussed:
  - Why are we allowing these insecure devices on the Power grid and what can we do to prevent that?

- Matter of time and dedication
- Problem is only getting worse…

New Insights

- Various other devices & brands also vulnerable
- +/- 4GW should be enough
  - Massive outage, very little can be done to counter this effect.
- Blueborne exploit?!
- Relative “Legacy” ?!
- Attention at all levels
  - Ongoing discussion and talks
  - Some evidence that things are changing in practice
  - Still a problem
    - Is becoming a bigger problem…

Other things…

- Bug bounty?
  - Paypal donations to w.westerhof.linkedin [at] (this.part.is.to.confuse.sp@m.bots) hotmail.com
- Want/need details?
  - Contact me via e-mail or linkedIn.
  - https://horusscenario.com/cve-information
    - Acknowledged, later on disputed when the press started asking questions…

Questions?


PRESENTATION FINISHED!
GOT ANY QUESTIONS?
memegenerator.net