Smart Energy 2017, Halden, Feb 2017

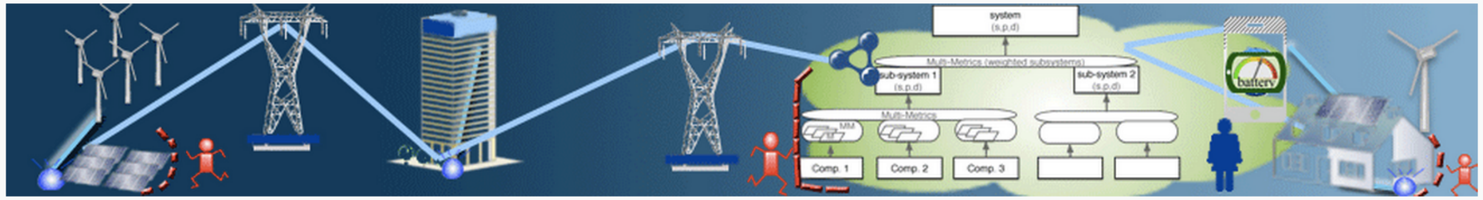
Industrial view - Smart Grid Security Centre

Otto Rustand
Glitre Energi Nett
IoTSec Security Officer
otto.rustand@glitreenerginett.no

National initiative for a more secure future in IoT

IoTSec.no - Security for IoT for Smart Grids

Home | Research Areas | Security Centre | Publications | About us



The **IoTSec - Security in IoT for Smart Grids** initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

Josef Noll @josefnoll 1 Nov

NCE Smart Partnerkonferansen @KristinHalvorsen og Nasjonal r for Sikkerhet i SmartGrid #IoTSec pic.twitter.com/FLLua94wlN

«Open World Approach»

everything that is not declared closed is open

Smart Grid Security Centre

Partners and Collaborations

Academia
- UiO
- UNIK
- NR
- Simula
- NTNU

Industry
- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

Interest Org.
- Smartgrid Centre
- Norw. Data Protection Auth.
- Forbrukerrådet

Industry
- EyeSaaS
- mnemonic

International
- Mondragon Unibersitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimbeo
- H2020 and ECSEL projects

SMARTGRID SECURITY CENTER

Handling of
Confidential and security-critical material

Retningslinjer på
http://cwi.unik.no/wiki/IoTSec:Secure_and_Confidential_information

Confidential information [edit]

- Documents which are given to the project being confidential to the project shall be watermarked by *IoTSec confidential, shall not be distributed outside of the project without consent"*
- Deliverables being confidential shall be stored on the project server, e.g. owncloud.unik.no

Security-critical information [edit]

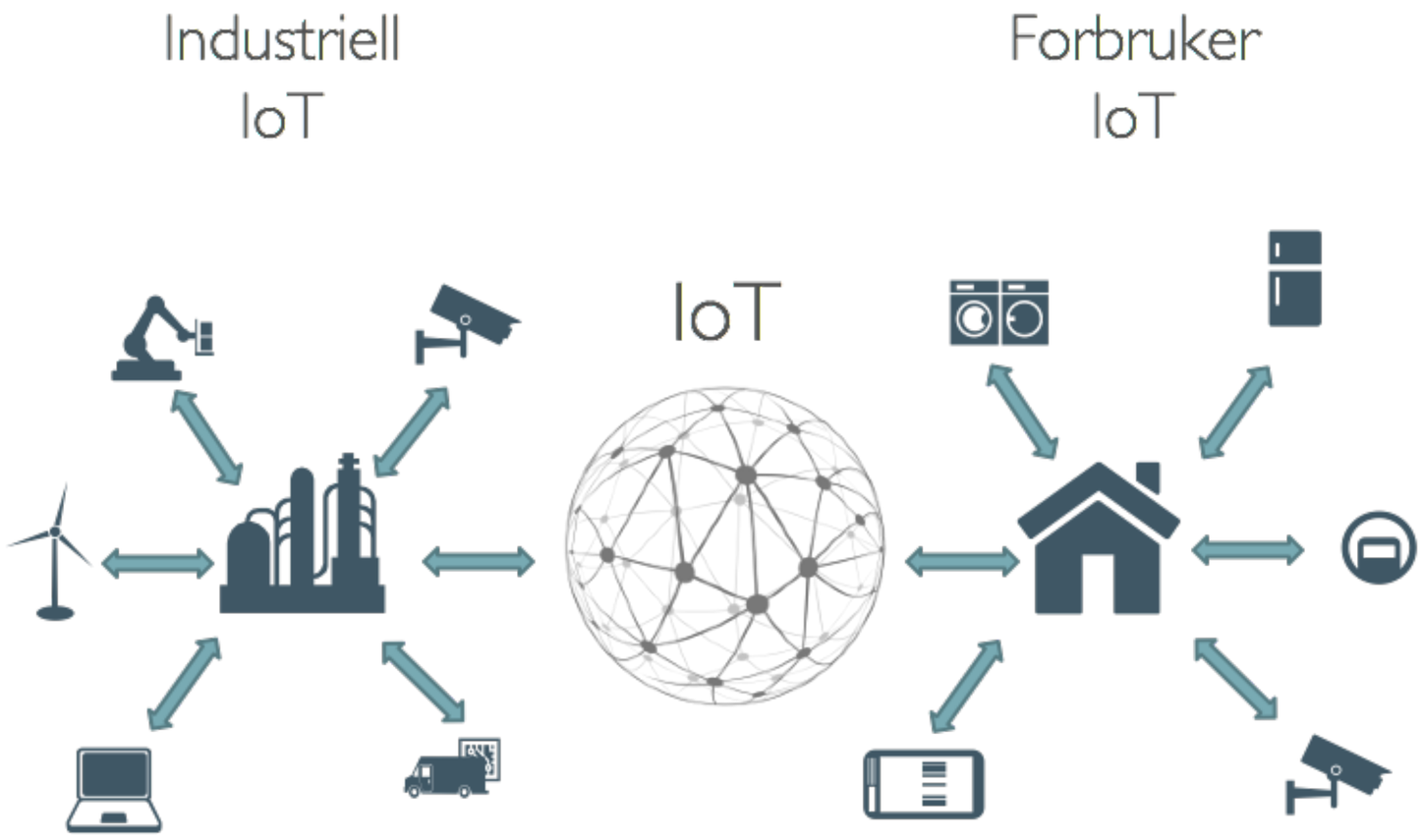
Each project participant is asked to not publish security-critical information. If a participant regards information as potentially security-critical, he shall ask IoTSec's security officer for advice.

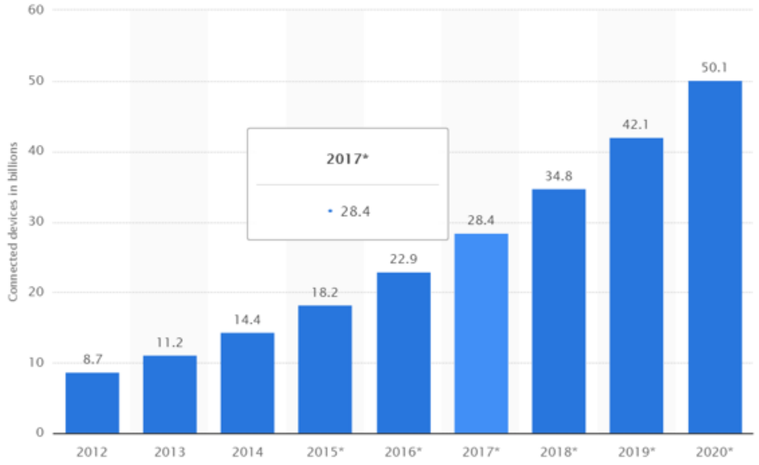
We have to follow the rules from NVE, outlining the rules and regulations, see Action Item to address NVE rules and regulations. The rules include a.o. a non-disclosure agreement for certain information.

Security critical information shall be watermarked "security-critical - do not distribute", and shall only be given to project partners on request. The distribution shall be noted to our COO (Christian Johansen), who keeps a list of the documents and whom they have been distributed to.

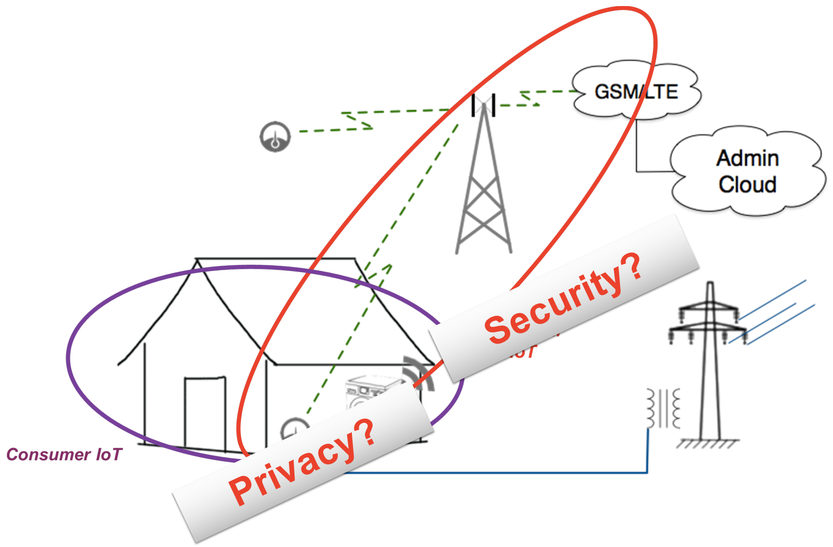
The IoTSec security officer is **Otto Andreas Rustand**, ask him for advice.

Industrial view versus Consumer view





The challenges - Smart Grid vs Smart Home



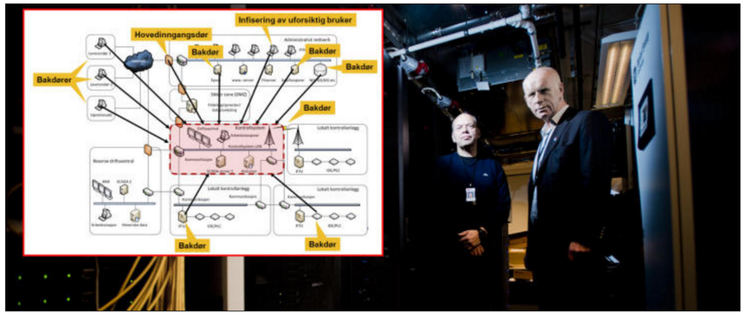
Smart Grid
- *Limited public knowledge*
- Security by *design*
- Security is the responsilbilty of supplier

Smart Home
- *«Wild West» of devices*
- «Plug and play»
- Limited user knowledge
- *Limited security awareness*

Smart home services

[Source: https://www.samsungsds-nss.com/?p=en_smarthome_private

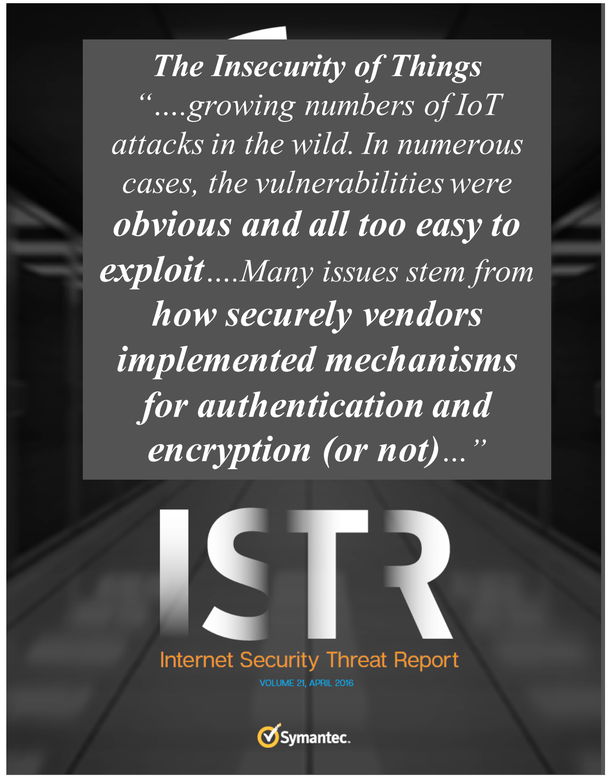
Treaths

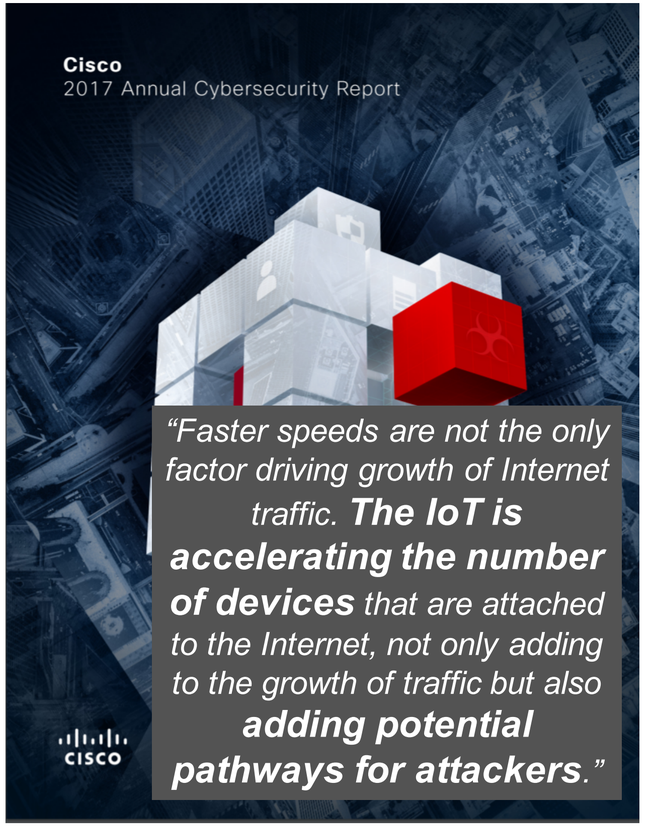


- Denne typen tiltak gjør oss mer sårbare for ondsinnede angrep

dn tv NVE advarer om nye trusler mot strømnettet. Les mer

Trends in security





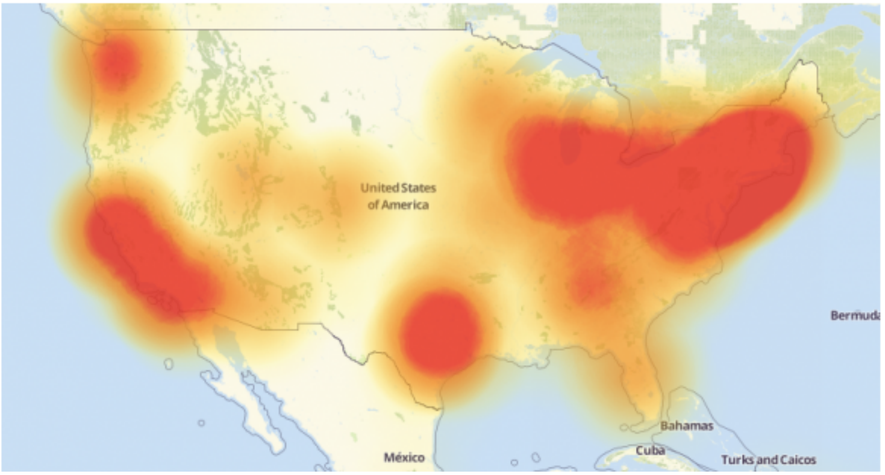
Treath examples

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



[Source: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/]

Computing

Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Russian hackers may be behind attacks leveled at the nation's power grid and artillery. The West should take note.

by Jamie Condliffe December 22, 2016

[Source: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

IoTSec Movie

http://www.iotsec.no

SMARTGRID SECURITY CENTER

Samarbeid basert på tillit

- Industriell perspektivet
- Samarbeid for å øke tillit
  - ➡ blant aktører
  - ➡ til forbrukeren
- Samarbeid for å øke sikkerhet
  - ➡ samfunnssikerhet
  - ➡ forsyningssikkerhet
- Utdannelse fra Akademia

Simulasjon
Nettovervåking
Proaktiv Maintenance

IKT sikkerhet
IoT sikkerhet
Penetration testing

Møteplass
Kunnskapsbase
IoT kommunikasjon

SMARTGRID SECURITY CENTER

Glitre Energi, FEN, …
Smart Innovation
Mnemonic, ….

Energi Norge
KraftCert
Norwegian Smartgrid Center

NVE, Datatilsynet, Forbrukerrådet
Akademia
UiO, NTNU, UiA
Forskningsinstituter NR, Simula, …

Mission Statement

We help the Utility Companies achieve their smart grid goals with higher resiliency and quicker response times against security threats.

SMARTGRID SECURITY CENTER