Industrial view - Smart Grid Security Centre

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

«Open World Approach»
everything that is not declared closed is open
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 not to 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 responsibility of supplier

Smart Home
- "Wild West" of devices
- "Plug and play"
- Limited user knowledge
- Limited security awareness
Smart home services

[Source: https://www.samsungds-nss.com/?p=en_smarthome_private]
- Denne typen tiltak gjør oss mer sårbare for ondsinnede angrep

[Image: NVE adværer om nye tilnærmelsel. Læs mer]
Trends in security

"The Insecurity of Things "....growing numbers of IoT attacks in the wild. In numerous cases, the vulnerabilities were obvious and all too easy to exploit. Many issues stem from how securely vendors implemented mechanisms for authentication and encryption (or not)...."

"Faster speeds are not the only factor driving growth of Internet traffic. The IoT is accelerating the number of devices that are attached to the Internet, not only adding to the growth of traffic but also adding potential pathways for attackers."
**21 Hacked Cameras, DVRs Powered Today’s Massive Internet Outage**

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.

**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/]

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

Smart Grid Security Centre
IoTSec Movie
http://www.iotsec.no
Samarbeid basert på tillit

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

Simulasjon
Nettovervåking
Penetration testing
IoT sikkerhet
Proaktiv Maintenance
Møteplass
Kunnskapsbase
IoT kommunikasjon

Samarbeid for å øke tillit
.edges
blant aktører
til forbrukeren

Samarbeid for å øke sikkerhet
.samfunnssikkerhet
forsyningssikkerhet

Utdannelse fra Akademia

Glitre Energi, FEN, ...
Smart Innovation
Mnemonic, ...
Energi Norge
KraftCert
Norwegian Smartgrid Center
NVE, Datatilsynet, Forbrukerrådet
Akademia
UiO, NTNU, HIA
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.