IoTSec Steering Board Meeting, 26Oct2016

Y1 Reporting

Christian Johansen
UiO/Ifi & UNIK
christi@ifi.uio.no

Josef Noll
UiO/UNIK
josef@unik.no

#IoTSec, #IoTSecNO

Agenda Styremøte IoTSec

Orienteringssaker

I • Kort informasjon om status etter 1. år i prosjektet

II • Forberedelse til møte med Forskningsrådet 23Nov2016, kl 1130-1530, særlig: innspill til NFR til fokus på research

III • Styrearbeid: møte, styremedlemmer, ++

Beslutningssaker

III • Valg av styrets leder

IV • Arbeidspakkeledelse og forventete resultater (deliverables,++)

V • Behandling av sikkerhetsrelevante informasjon

Project Info - Y1 highlights

- 2 PhD and 3 PostDoc positions are filled, offer for the final PhD position was accepted
- Consolidated plans for Smart Grid Security Centre are established.
- Extended Collaboration with Groups and Initiatives, grown from 11 to 19 partners
  - ➡ UiA joined, and 6 external professors (UiA, UiO/Simula, Chalmers, Univ Copenhagen)
- EU Horizon 2020 project INVADE accepted
  - ➡ coordinated by IoTSec partner NCE Smart, with 3 partners from IoTSec
- JU ECSEL project proposal SCOTT submitted as IA,
  - ➡ with UiO as Technology Leaders and Norwegian consortium coordinator, 7 Norwegian partners
- Strategic Research Partnership of UiO with the Virtual Vehicle Research Centre (Austria) on security and digital systems
- Dieter Hirdes got awarded by EU Energy Group, Josef by Virtual Vehicle Research Centre in Austria

Y1 highlights in measurable outcome

see: http://IoTSec.no/publications

- Scientific outcome
  - ➡ 4 conference contributions
  - ➡ 1 anthology
  - ➡ 4 journal contributions
  - ➡ 1 special issue co-editor
- Masterstudents
  - ➡ 3 ongoing, 1 finished, 9 open topics
  - ➡ 2 new courses
    - IoT Security (UNIK) and Energy Informatics (Ifi) plus one existing course
- Dissemination
  - ➡ 13 Presentations given, including Smart Grid Conf, Nemko, Sintef, NCE partner forum
  - ➡ dedicated face to face meetings with other actors like Hafslund, Agder Energi, Eidsiva Energi and Kragerø Energi
  - ➡ Twitter channels, Web page

- Excellent growth of scientific network
- Good Scientific outcome,
- Good involvements of students

- Excellent success rate of novel projects

Challenges

Scientific challenges

- missing descriptions of distribution grid
  - ➡ “security by obscurity”
  - ➡ different security viewpoint

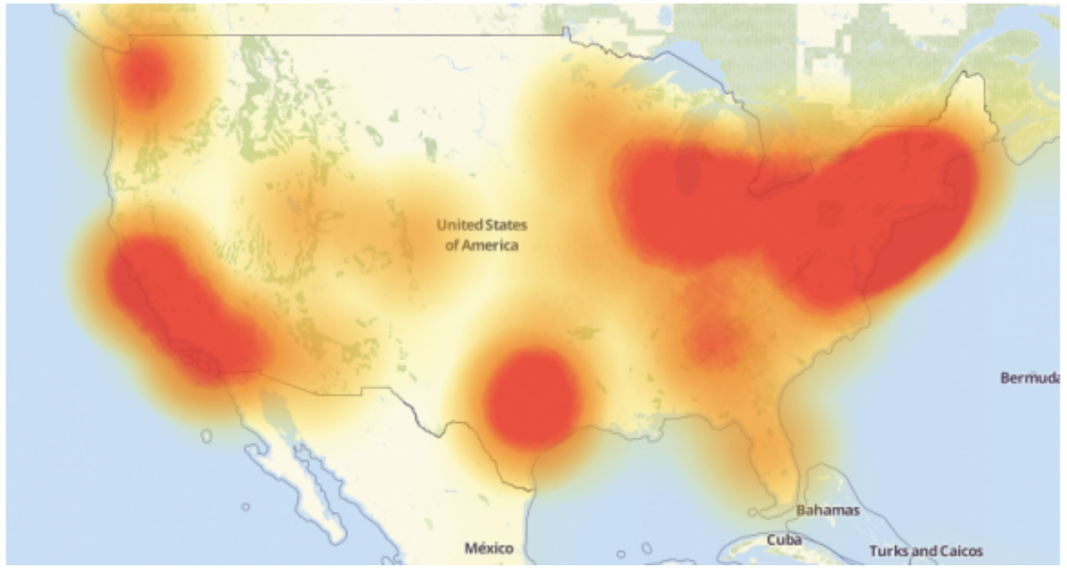
Collaboration challenges

- Academic versus industrial viewpoint
  - ➡ “language missmatch”
  - ➡ Academic: long term, open available information, e.g. Smart Home focus
  - ➡ Industry: current challenges, e.g. focus on grid
- Focus on Smart Grid Security Centre (SGSC)
  - ➡ Expected contributions
  - ➡ Academia has focus on science

21 OCT 16 Hacked Cameras, DVRs Powered Today’s Massive Internet Outage *16Oct2016*

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.

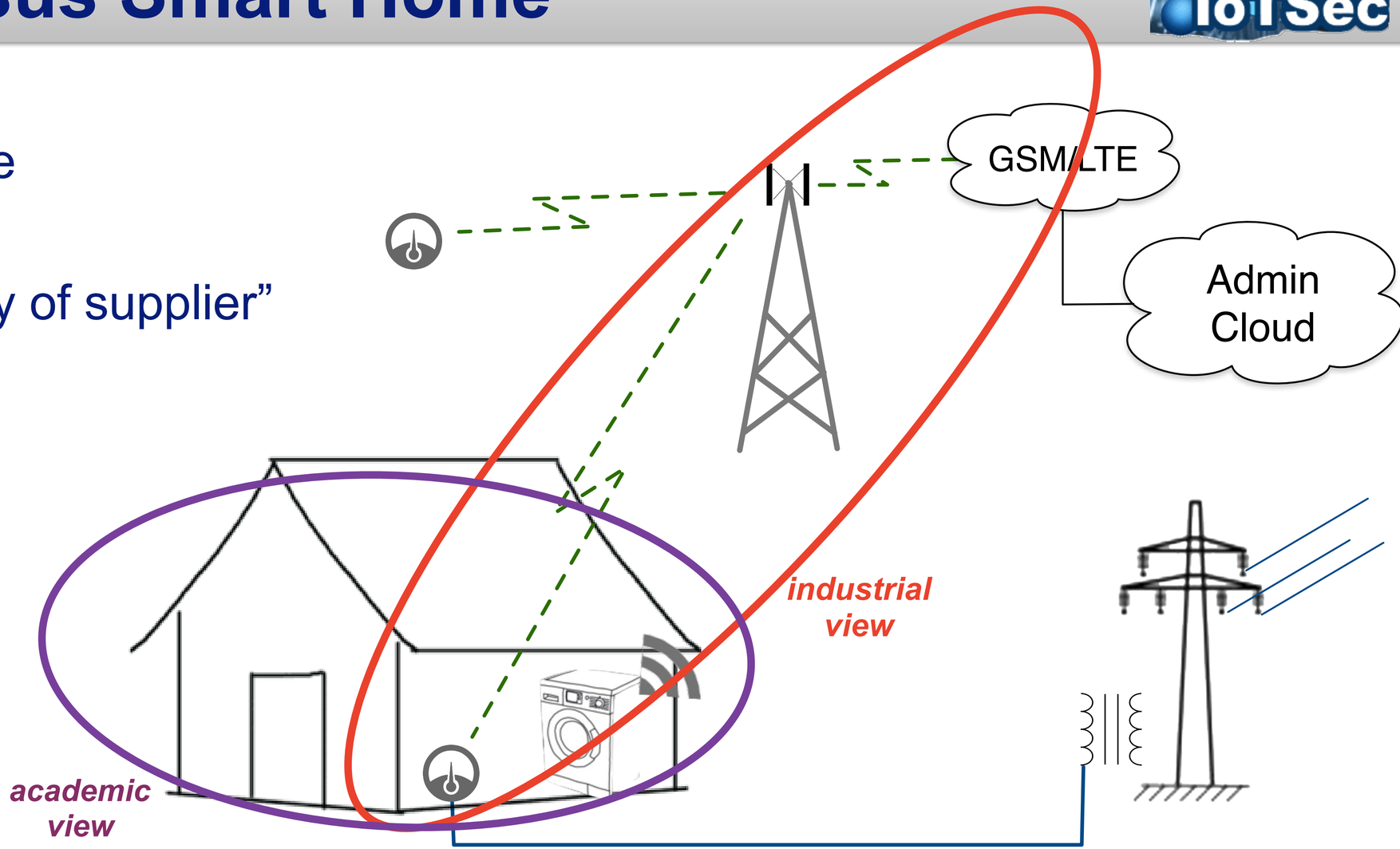
Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter,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



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

Visualisation - the challenges
Smart Grid versus Smart Home

- Smart Grid
  - ➡ limited public knowledge
  - ➡ “security by obscurity”
  - ➡ “security is responsibility of supplier”
- Smart home
  - ➡ tons of papers
  - ➡ interesting topics



Preparation:
Y1 Status meeting with Research Council 23Nov2016

Research Council asked for ideas on future research

- **Privacy labelling:** We have identified privacy labelling as a potential for making privacy work into a commercially viable alternative for companies that put more privacy into their products, apps, services. These can be seen for privacy the same as the energy labels for electronic equipment.
- **Regulations and policies**: Development in this area is going to be so fast that we need closer collaboration with regulative bodies.
- **User-involvement**: Research should be directed more towards the society, towards people. Incorporate citizens in projects, give them power to participate.
- **Early design**: Use of fast prototyping and visualisation as a tool for reducing research cost. When ideas are tested in early stage, critical mistakes may be avoided, thus saving resources.

Research specific challenges

- **Complexity** due to the concurrency and distributed nature of IoT systems
- **Context-centric computation**, since the IoT devices, e.g., in the Smart Home, must be aware of the humans
- **Lack of semantics**, since IoT systems would produce large amounts of data, which need semantic information in order to become usable.
- **Models vs. programs**: Analysis and evaluation for agile prototyping based on executable models and semantic-based tools, as and evolution from programming and their low-level tools.
- **Semantics for Security and Privacy**: Semantic technologies and ontologies are need to establish a unified terminology for fields of privacy and security. This would provide machine-readable data and would allow development of more automated tools.
- **Edge and fog** computing for privacy
- **Measurable security and privacy**: might sound unrealistic for some of the purist researchers in security, but this is what companies do every day, maybe under different names such as risk analysis. However, we see a lack of automated tools and methodologies to help in measuring such important “unmeasurable” aspects like security, privacy, or robustness, which are essential in evaluating smart infrastructures.
- your input?

Diskusjon og beslutning: Samarbeid i styret

Styrerepresentanter:

- UiO: Olaf Owe
- UNIK: Stian Løvold
- NTNU: Nils Kalstad Svendsen(?), Sofie Nystrøm(?)
- NR: Åsmund Skomedal
- Simula: Yan Zhang(?)
- NCE Smart: Dieter Hirdes
- eSmart Systems: Davide Roverso(?), Erik Åsberg(?)
- Glitre Energi Nett: Otto Andreas Rustand
- Fredrikstad Energi Nett: Vidar Kristoffersen
- Movation:Bjarne Haugen

Prosjektleder:

- Josef Noll
- Christian Johansen, COO, sekretær i styret

Styret:

- Møtefrekvens
- Temaer

Beslutning:

- N.N. er valgt som styrets leder

Bjarne Haugen er valgt som styrets leder

IV Beslutningssak: Arbeitspakkeledelse og forventete resultater

Bakgrunn

- Prosjektet ble etablert som forskerprosjekt
- Fokus i søknaden er rettet mot å etablere et Smart Grid Security Centre
- Oppgavefordeling for enhver partner ble beskrevet på Wiki, men prosjektlederen mangler en proaktiv tilnærmelse

Forslag til styrebeslutning:

Et sentralt mål til IoTSec prosjektet

- ~~xxxxx~~ Målet til IoTSec prosjektet er å etablere et Smart Grid Security Centre. Alle partner bes om å bidra aktiv til at forskningen blir tilpasset sikkerhetssenteret.
- Prosjektlederen er bedt til å informere styre om evtl avvik fra planen

V Beslutningssak: Konfidensiell og sikkerhetskritisk informasjon

Bakgrunn

- Prosjektet arbeider etter "open world assumption", dvs. all informasjon er offentlig hvis den er ikke betegnet som konfidensiell eller sikkerhetskritisk
- Prosjektet har etablert en åpen Wiki IoTSec.no og en konfidensiell Wiki admin.IoTSec.no
- Rutiner på behandling av konfidensiell og sikkerhetskritisk informasjon er etablert på: http://cwi.unik.no/wiki/IoTSec:Deliverables *(next page)*

Forslag til styrebeslutning:

- Styret støtter **initielle** retningslinjer om bruk av konfidensiell og sikkerhetskritisk informasjon (dokumentert 26Okt2016)
- ~~Styret foreslår n.n. som IoTSecs Security Officer~~ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Styret bes prosjektet til å jobbe videre med saken

Otto deler ….

Bakgrunn:
Konfidensiell og sikkerhetskritisk informasjon

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

Confidential and secure information [edit]

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-relevant 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.

The IoTSec security officer is **n.n.**.

grids

1. Next-generation energy storage: the project at glance

World's population is increasing and with it the amount of energy needed. Today's confluence of challenges – rapidly escalating global energy demands and wide access to energy sources – demand innovative way of thinking to forge a pathway to a sustainable energy future. According to recent projections, in order to achieve climate change targets of 80-90 percent reduction of the greenhouse gas carbon dioxide from the power sector, Europe is aiming to increase to 90 % or more the penetration of renewable energy in 2050. With the current status of electricity distribution grid, the new scenario would require a significant transmission lines addition (so called grid extension) in order to spread resources over large areas. This will have a strong impact on our landscape and will not solve the problem of energy losses for conversion from alternating to direct current (AC/DC). Beyond penetrations of 30% the variable generation supply and demand will impose increasing scientific challenges and will require additional enabling technologies such as energy storage.

The last decades the scientific community focused on developing Li-based batteries for portable and vehicular applications, due to their high energy and power capabilities. However, concerns are rolling over Li availability facing a future demand for batteries with requirements different from the portable electronics, for example for large scale applications such as the electricity grid. Transforming the energy grid will require innovative ideas for energy storage systems and major breakthroughs in materials discoveries.

In the present proposal, I suggest an innovative concept of how the future grid could be. My vision is decentralizing the energy generation and distribution, where the electricity produced through renewable sources by a single house, or small/medium communities, would be stored in a novel concept of stationary batteries able to exchange electricity and information with the grid in an "intelligent" manner. Thus, the main aim of the current proposal is to develop Na-ion based batteries for stationary storage device for integration of renewable energy in smart grid applications. The new battery will use inorganic nanotubes and porous nano-composites to make the electrodes denser in terms of energy capacity than other existing batteries. The choice of sodium, instead of lithium addresses the availability and toxicity issues of the materials. Additionally, the new proposed storage device will require modeling the security and the exchange of information with the grid about the type of renewable energy used, the energy capability of the network, and the profile usage of the client.

To achieve this, three main hypothesis are put forth:

1) Sodium can replace lithium in next-generation energy storage materials for large scale applications

2) Nanocomposites architectures in the electrodes in the form of nanoconfined materials and inorganic nanotubes will enhance the mass diffusion and electron transfer increasing the accessibility of the active material

3) Future grid will allow a higher penetration of renewables and empowering consumers through energy storage units. A new communication system between the storage units/customers and the grid will allow an increase flexibility of the grid and protection of private information.

In the next pages I will explain how these hypothesis will be tested. But first I will describe shortly how SmartStorage fits into the bigger picture of global energy demands.

2. Future growth in demand of wind and solar photovoltaic energy means growing need of storage capacity

A fundamental challenge to significantly integrating renewable-generated power sources – such as wind and sun – into the electric grid is their inherent variability.

This challenge makes electricity storage critical and, I believe, the next frontier in energy infrastructure.

AOB

- Any other business?

ikke noen

- Next meeting,

i sammenheng med sikkerhetsarbeidet

  ➡ to be called in by the steering board leader?