Atle Årnes

Fagdirektør teknologi

Datatilsynet

Regelverk for IoT

- GDPR
- ePrivacy

Tillit

- Bruken av IoT både fra forbrukernes side og organisasjonene er basert på tillit.
- Tillit med tanke på sikkerhet, åpenhet rundt bruk av data, tydelig informasjon etc.

IoT på 5G

- Alt på nett og 5G virkeliggjør det og gjør det raskere.

- 5G vil flytte prosessorkraften vekk fra lokalt utstyr og ut i skyen. Små, strømgjerrige prosessorer vil være over alt – mens intelligensen vil ligge i skyen, takket være høye overføringshastigheter og lavere responstid.

- Alt kan ha sensorer og alt kan være på nett. Og alt forteller om temperatur, lokasjon, osv.

4G og 5G

GSMA Intelligence Mobile World Live

MENU

Narrow Band – Internet of Things (NB-IoT)

Low Power Wide Area

1. Veldig lavt strømforbruk. Batterilevetid på år og over 10 år fon noen løsninger.
2. Optimalisert for korte meldinger– som lengden på en SMS.
3. Veldig lav kostnad pr enhet– kommunikasjonsenheten vil eventuelt koste noen “few dollars”.
4. Ha god dekning bade innendørs og utendørs I områder som tidligere ikke kunne nås, utenfor dekning for strømkilder.
5. Være lette å koble til eksiterende nettverk, gjenbruk av mobilnett der dette er mulig.
6. Skalerbare ved å kunne håndtere et stort antall enheter over et stort geografisk område.
7. Levere ende til ende sikker kommunikasjon og håndtere atutentisering som passer IoT-løsningen.
8. Gi mulighet for å bli integrert med en mobiloperatørs enhetlige IoT platform.

- Enormt mange fordeler. Fjernkirurgi og helsesesensorer
- Vs
- Svindel og overvåking

GDPR-problematikk

- Nytt personvernregelverk er forholdsvis tilbakeholdent når det gjelder tekniske krav.

Art 32 Sikkerhet ved behandlingen

- Behandlingsansvarlig og databehandleren skal gjennomføre tiltakene for å ivareta sikkerheten
- Risikovurdering
- Overholde bransjenormer
- Avvikshåndtering

Tiltak i hht Art-32 – Sikkerhet ved behandlingen

- Pseudonymisering og kryptering av personopplysningene.
- Sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og –tjenestene.
- Evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.
- En prosess for regelmessig prøving, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

GDPR og IoT

- Innskjerping av avvikshåndtering
- Hvordan innhente korrekt samtykke?
- IoT og barn.
- Big data, IoT, roboter og kunstig intelligens er sammen om å fremme regulering.
- IoT forutsetter tillit og åpenhet.

Oppdatering av IoT

- Oppdatering er nødvendig for å
- Gi ny funksjonalitet
- Rekonfigurering på grunn av endrede internetprotokoller
- Fjerning av bugs (patching)
- Svak kryptering eller nøkler må byttes.

Personvernutfordringer

- Kan gi en angriper direkte tilgang til en sensor, for aktivering og hente data.
- IoT-enheten kan gi tilgang til brukernavn og passord til e-postkontoer, sosiale nett osv.

Man må:

- Fremme utviklingen og bruk av oppdatering av firmware.
- Fremme prosjekter som setter fokus på sårbarheter.
- Sette krav til sikkerhet for IoT-utstyr, hvor
  - Det gis info om installert firmware
  - Info om håndtering av firmware og frister for oppdatering.
  - Hva sluttbrukeren kan gjøre.

Oppdatering av firmware, problematikk

1. IoT-enheter er ikke alltid lett tilgjengelige
2. Enheten kan kanskje ikke oppdateres, men bare byttes
3. Alle IoT-ehetene oppdateres ikke samtidig
4. Hvem eier enheten og er ansvarlig
5. Informasjon om at ny firmware er tilgjengelig
6. Firmware kan uønsket endre funksjonalitet på IoT-enheten
7. Oppdateringen kan feile
8. Delvis oppdatering feiler
9. Sårbar for svindel-firmware
10. Produsent slutter å levere oppdateringer
11. Isolering av ikke-oppdaterte IoT-eheter
12. Tuklete oppdatering medfører at oppdaterig unnlates.

Personvern og risiko

- Sårbarheter i firmware kan gi angripere tilgang til sensorer
- Angripere vil prøve å utnytte sårbarheter
- Angripere vil prøve å bruke en enhet som proxy til en annen.
- IoT enheten kan ha lagret data som er hentet over tid, disse data kan hentes ned raskt
- IoT-enheten kan uønsket avdekke krypteringsnøkler.
- IoT-enheten kan avdekke passord til andre tjenester som f.eks. E-post og sosiale nettsamfunn.

For myndigheter

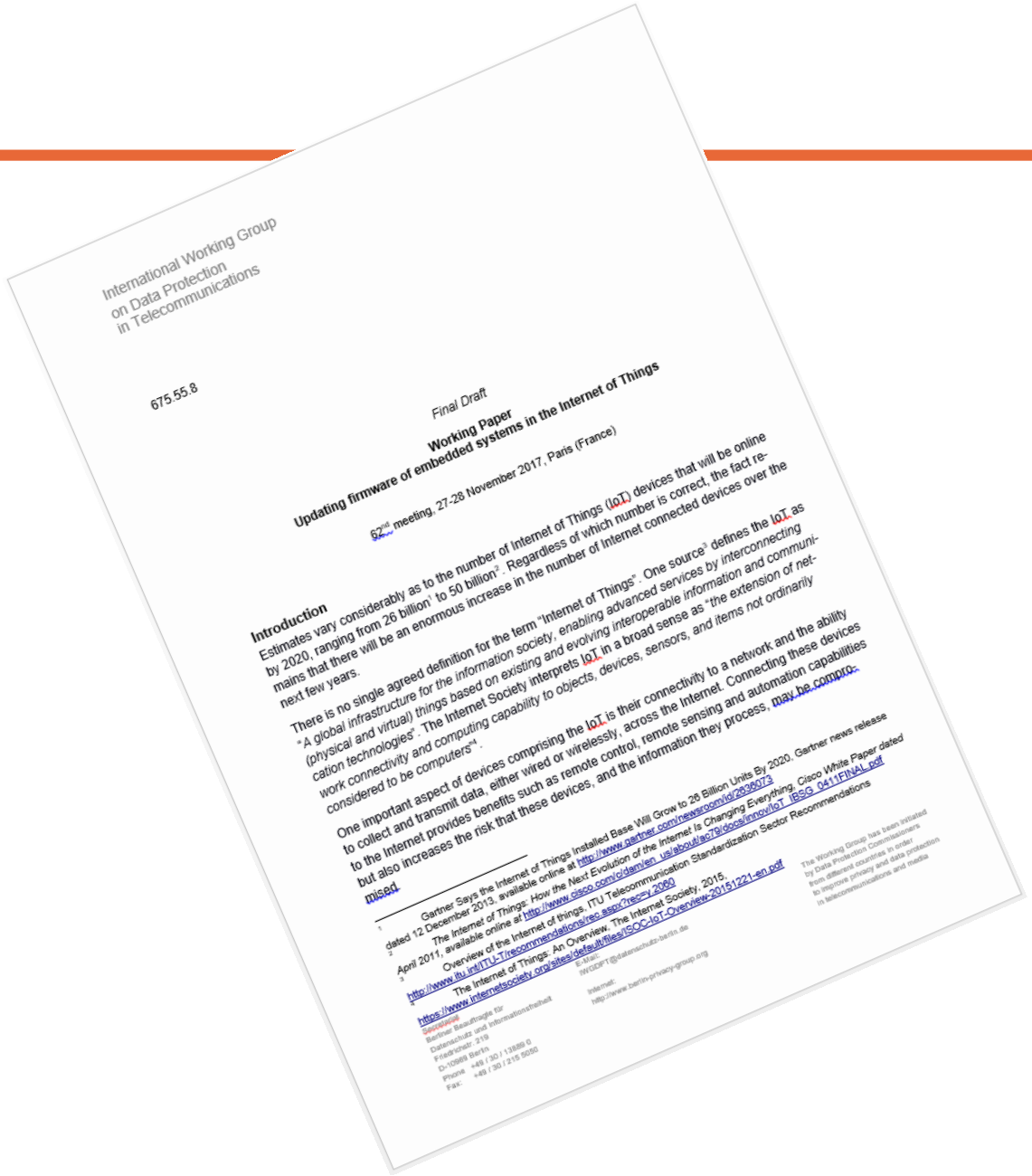
- Fremme felles mekanismer for firmware oppdateringer.
- Fremme utdanningen av virksomheter og folk vedrørende distribusjon av firmware oppdatering
- Fremme prosjekter som adresserer sårbarheter på IoT
- Sette krav til markedet for IoT
- Sette krav til sertifisering av IoT firmware

For produsenter

- Utvikle sikker firmware
- Utvikle automatiske og personvernvennlige oppdateringer
- Avklaringer om integritet på firmware oppgraderingen
- Levere tilstrekkelig informasjon
- Bruke åpne standarder
- Benytte korrekte anbefalinger for sikkerhet og personvern
- Opplyse om når sikkerhetsoppdateringer avsluttes
- Gi oppdateringer når de trenges
- …

Ytterligere anbefalinger for:

- Eiere av IoT-enheten når dette er organisasjoner
- Eiere av IoT-enheten når dette er enkeltpersoner



International Working Group
on Data Protection
in Telecommunications

675.55.8

Final Draft

Working Paper

Updating firmware of embedded systems in the Internet of Things

62nd meeting, 27-28 November 2017, Paris (France)

Introduction

Estimates vary considerably as to the number of Internet of Things (IoT) devices that will be online by 2020, ranging from 26 billion[1] to 50 billion[2]. Regardless of which number is correct, the fact remains that there will be an enormous increase in the number of Internet connected devices over the next few years.

There is no single agreed definition for the term "Internet of Things". One source[3] defines the IoT as "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*". The Internet Society interprets IoT in a broad sense as "*the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers*"[4].

One important aspect of devices comprising the IoT is their connectivity to a network and the ability to collect and transmit data, either wired or wirelessly, across the Internet. Connecting these devices to the Internet provides benefits such as remote control, remote sensing and automation capabilities but also increases the risk that these devices, and the information they process, may be compro-

mised

1 Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, Gartner news release dated 12 December 2013, available online at http://www.gartner.com/newsroom/id/2636073

2 *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper dated April 2011, available online at http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

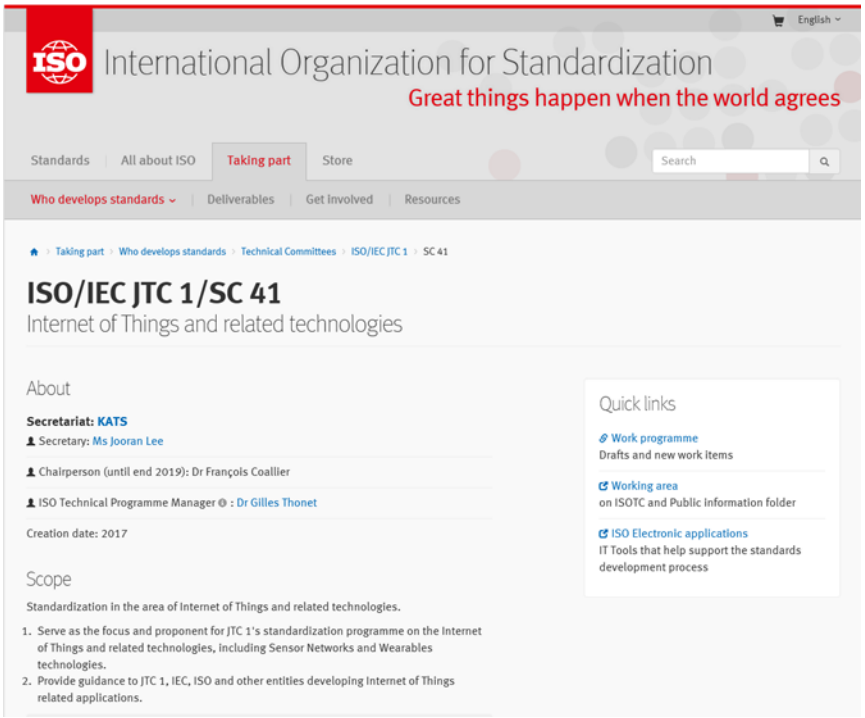
3 Overview of the Internet of things, ITU Telecommunication Standardization Sector Recommendations http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

4 The Internet of Things: An Overview. The Internet Society, 2015. https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone: +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050
E-Mail: IWGDPT@datenschutz-berlin.de
Internet: http://www.berlin-privacy-group.org

The Working Group has been initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media

Internet of Things and related technologies



Standard and/or project under the direct responsibility of ISO/IEC JTC 1/SC 41 Secretariat (20)

ISO/IEC 19637:2016
Information technology -- Sensor network testing framework

ISO/IEC 20005:2013
Information technology -- Sensor networks -- Services and interfaces supporting collaborative information processing in intelligent sensor networks

ISO/IEC CD 20924 [Under development]
Information technology -- Internet of Things (IoT) -- Definition and vocabulary

ISO/IEC AWI 21823-1 [Under development]
Internet of things (IoT) -- Interoperability for internet of things systems -- Part 1: Framework

ISO/IEC TR 22417:2017
Information technology -- Internet of things (IoT) use cases

ISO/IEC TR 22560:2017
Information technology -- Sensor networks -- Use cases of aeronautics industry: Active Air-flow Control

ISO/IEC 29182-1:2013
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 1: General overview and requirements

ISO/IEC 29182-2:2013
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 2: Vocabulary and terminology

ISO/IEC 29182-3:2014
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 3: Reference architecture views

ISO/IEC 29182-4:2013
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 4: Entity models

ISO/IEC 29182-5:2013
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 5: Interface definitions

ISO/IEC 29182-6:2014
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 6: Applications

ISO/IEC 29182-7:2015
Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 7: Interoperability guidelines

ISO/IEC 30101:2014
Information technology -- Sensor networks: Sensor network and its interfaces for smart grid system

ISO/IEC 30128:2014
Information technology -- Sensor networks -- Generic Sensor Network Application Interface

ISO/IEC DIS 30140-1.3 [Under development]
Information technology -- Underwater acoustic sensor network (UWASN) -- Part 1: Overview and requirements

ISO/IEC 30140-2:2017
Information technology -- Underwater acoustic sensor network (UWASN) -- Part 2: Reference architecture

ISO/IEC CD 30140-3 [Under development]
Information technology -- Underwater acoustic sensor network (UWASN) -- Part 3: Entities and interface

ISO/IEC CD 30140-4 [Under development]
Information technology -- Underwater acoustic sensor network (UWASN) -- Part 4: Interoperability

ISO/IEC CD 30141 [Under development]
Internet of Things Reference Architecture (IoT RA)


Kamstrup
12861 kW
KAMSTRUP 382M4G
Made in Denmark


Kamstrup
Ultrasonic
Water meter
DK-8660
63123453
00587 263
m³
LEAK BURST TAMPER
DRY REVERSE
FLOW
2032
MULTICAL® 21
Type: 02146A0H817
S/N: 63123453/00/16
Class: 2 (E2, M1)(B/C)
T50: 0.1°C...50°C
Q3: 2.5 m³/h
Q3/Q1: 250, SW:N1
PN16, PS16 - IP68
CE M16 0200
DK-0200-MI001-015

Veileder

Programvareutvikling med innebygd personvern

Denne veilederen skal hjelpe norske virksomheter å forstå og etterleve kravet om *innebygd personvern* i de nye personvernreglene. Den er utarbeidet i samarbeid med sikkerhetseksperter og programutviklere i privat og offentlig sektor. Veilederen har også vært på høring i flere virksomheter og organisasjoner.