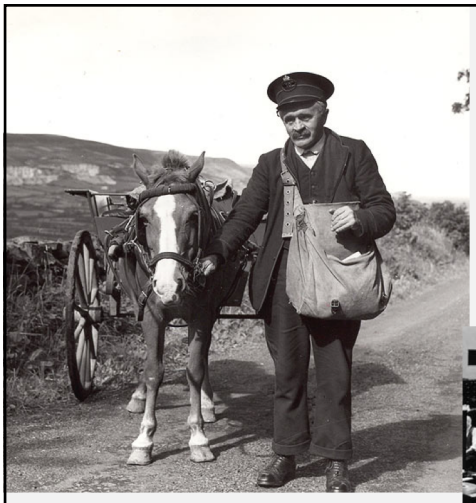
Lawful interception of Internet Traffic, and national autonomy in cyberspace

Olav Lysne
Professor
Simula Metropolitan

Simula Research Laboratory AS



3

Mobile payment

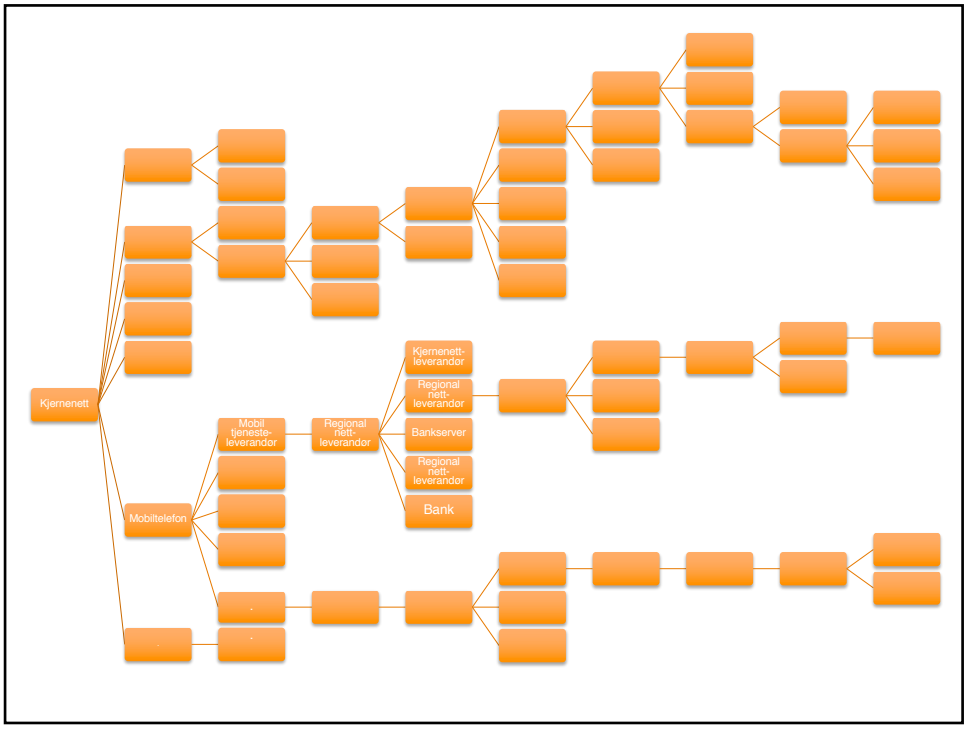
Payment app
Mobile phone
Mobile service provider
Regional network provider
Nation wide network provider
Regional network provider
Bank server
Regional network provider
Nation wide network provider
Regional network provider
Bank server

Mobile payment

Payment app
Mobile phone
Mobile service provider
Regional network provider
Nation wide network provider
Regional network provider
Bank server – value chain for authentication
Regional network provider
Nation wide network provider
Regional network provider
Bank server – value chain for authentication

Mobile payment

Payment app
Mobile phone
Mobile service provider – operation outsourced
Regional network provider – operation outsourced
Nation wide network provider – operation outsourced
Regional network provider – operation outsourced
Bank server – value chain for authentication
Regional network provider – operation outsourced
Nation wide network provider – operation outsourced
Regional network provider – operation outsourced
Bank server – value chain for authentication



Properties of digital value chains

Faults propagate instantly, and sometimes in unpredictable ways.

The services that constitute a value chain span multiple sectors, and are subject do different regulative regimes.

For those developing a service on top of such value chains, it is very challenging to get an overview of the inherited vulnerabilities throughout the value

Some services are at the bottom of a very large number of value chains.

Almost all sectors facing the same challenges

They are in the midst of a profound technologically driven transformation

Enthusiasm of technology mixed with alienation to risk

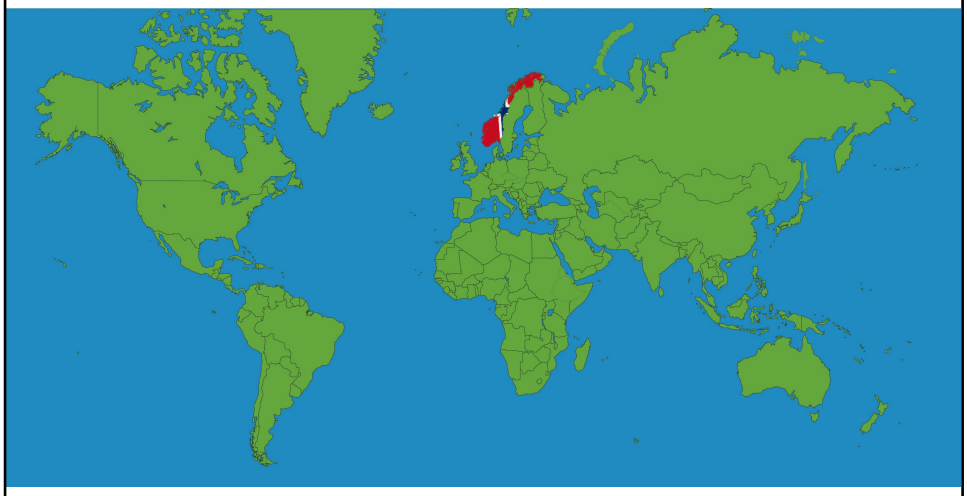
Workforce with yesterday's competence

Management lacks background to comprehend the hazards, understand the remedies and evaluate residual risk

Regulations adapted to former times

The criticality of Telenors core network needs to be reduced


Sweden
Norway
Finland
Faroe Islands
Oslo
Stockholm
Helsinki
St Petersburg
Tallinn
Estonia
Latvia
Riga
Lithuania
Vilnius
Minsk
Belarus
Moscow
Nizhny Novgorod
Kazan
Edinburgh
United Kingdom
Isle of Man
Dublin
Ireland
Manchester
Liverpool
London
Denmark
Hamburg
Amsterdam
Netherlands
Berlin
Poland
Warsaw
Germany
Cologne
Brussels
Belgium
Frankfurt
Prague
Luxembourg
Paris
France
Czechia
Slovakia
Vienna
Munich
Austria
Budapest
Hungary
Switzerland
Slovenia
Zagreb
Milan
Croatia
Bosnia and Herzegovina
Serbia
Belgrade
Monaco
Italy
Rome
Kosovo
Macedonia (FYROM)
Albania
Tirana
Greece
Bucharest
Romania
Moldova
Chisinau
Odessa
Ukraine
Kiev
Kharkiv
Voronezh
Saratov
Volgograd
Rostov-on-Don
Krasnodar
Black Sea
Istanbul
Bursa
Ankara
Turkey
Georgia
Armenia
Azerbaijan
Andorra
Barcelona
Porto
Madrid
Portugal
Lisbon
Spain
Valencia



Critical infrastructure

Norwegian Security Act (Sikkerhetsloven):
«anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner».

Civil Protection Act (Sivilbeskyttelsesloven):
«anlegg, systemer eller deler av disse som er nødvendige for å opprettholde sentrale samfunnsfunksjoner, menneskers helse, sikkerhet, trygghet og økonomiske eller sosiale velferd og hvor driftsforstyrrelse eller ødeleggelse av disse vil kunne få betydelige konsekvenser».

Can we still assume that all installations satisfying these definitions are located in Norway, overseen by Norwegian authorities, and governed by Norwegian Law?

Lawful Interception of Internet Traffic in Norway

Professor Olav Lysne

Digital Border Control/Lawful Interception

An installation that gives the Norwegian foreign intelligence service access to data from the Internet-cables crossing the Norwegian border.

Similar installations already exist in countries we like to compare ourselves to

- Sweden, Germany, France, Great Britain, USA and Canada
- Switzerland has approved legislation, and had a referendum with positive result
- Under consideration in the Netherlands and in Finland

The Norwegian Foreign Intelligence service have argued that they need it

The Lysne I commission argued that a new commission should write a report, followed by a public debate.

Etterretningstjenesten's mission

Foreign intelligence – civil and military

Obtain information of activities foreign states, organizations and individuals that are of relevance to Norwegian interests.

This information is intended for support of decisions taken by Norwegian authorities and Norwegian defence

The information is not intended for fighting crime

Etterretningstjenesten are not allowed to collect information on Norwegians residing in Norway.

Lawful interception - why now?

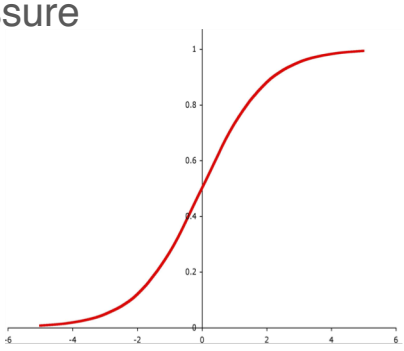
Changes in the threat landscape

- International cyber-attacks are escalating in complexity and in absolute numbers
- International terror is being coordinated over the Internet

Technological changes

- Earlier communication channels are being replaced by Internet-based services
- Older capacities for intelligence need be replaced

Privacy is under technological pressure



Privacy

What will be possible in 20 years?

What will be compromising in 20 years?

Is it possible to allow collection of big datasets, and later disallow?

Should we worry about a national coup?

The chilling effect-how strong is it?

Why is this difficult?

A large and increasing portion of the digital activity of Norwegians in Norway crosses our borders in the cables that will be intercepted.

A diminishing part of our lives are fully analogue. Most of our daily activities generate digital traces that cross the border

Access to the cables crossing the border gives access to information of the daily lives of Norwegians on an unprecedented scale.

This makes the question sensitive with respect to privacy, human rights, legality, and it challenges the relation of trust between the population and Etterretningstjenesten.

Lawful interception is only recommendable if it can be made

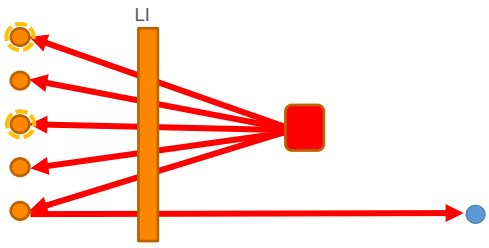
technologically feasible,

legally acceptable,

does not harm the relation of trust between the population and the authorities, and

gives valuable intelligence.

Valuable intelligence – meta-data and content- data



Metadata is stored over time, allows us to answer
When did the first attack occur?
Who else have been attacked?

Content data is retained when there is reasonable suspicion:
Allows us to analyse the attack technically

Valuable intelligence – meta-data and content- data

Foreign terrorist cell is discovered, and they are suspected to plan an

- Have any of them been communicating with someone in Norway lately?

We observe that they are moving

- Are they communicating with Norway, and if so, what are they saying/writing?

Technologically feasible

It is generally impossible to filter out only the information that is of relevance for foreign intelligence.

An implementation of LI will inevitably contain information that we would rather not that the Secret Services should have access to.

An implementation of LI will therefore need human and technical barriers for misuse.

Legally acceptable

Laws and conventions:

- Grunnloven, Personopplysningsloven, Lov og instruks om Etterretningstjenesten, EMK, FN-konvensjonen om sivile og politiske rettigheter, Europarådets personvernkonvensjon, Personvernsdirektivet/Personvernsforordningen ...

Interpretations

- Datalagringsdirektivet
- Privacy
- Big Brother Watch vs. UK
- The Tele2-case

We should not introduce LI, only to see it deemed illegal in court

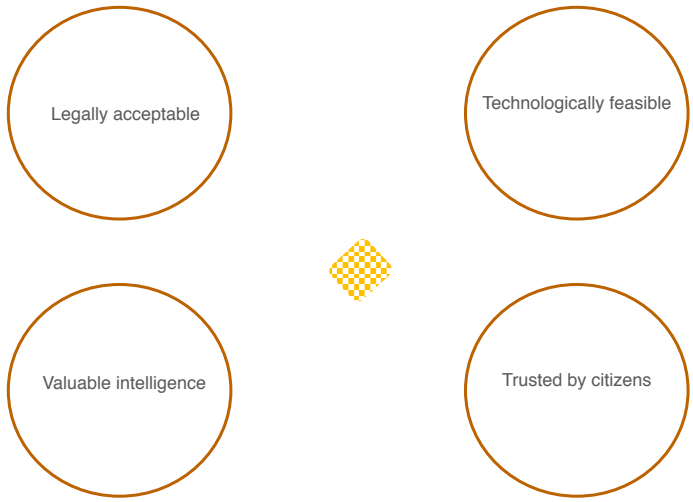
LI will most probably be tested in court

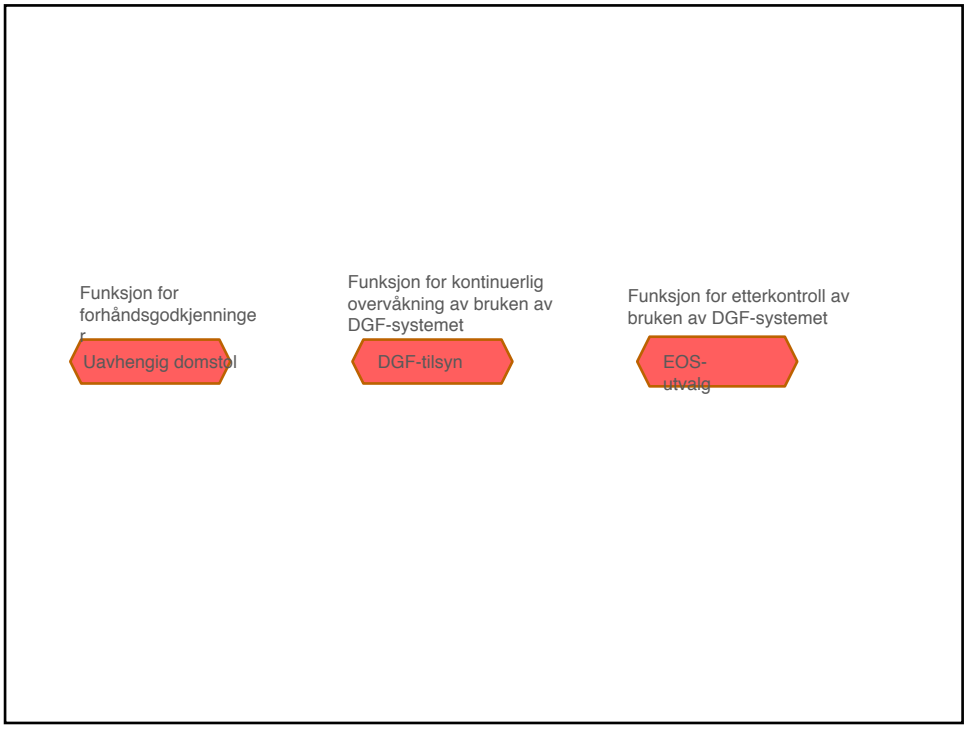
Maintain citizen trust

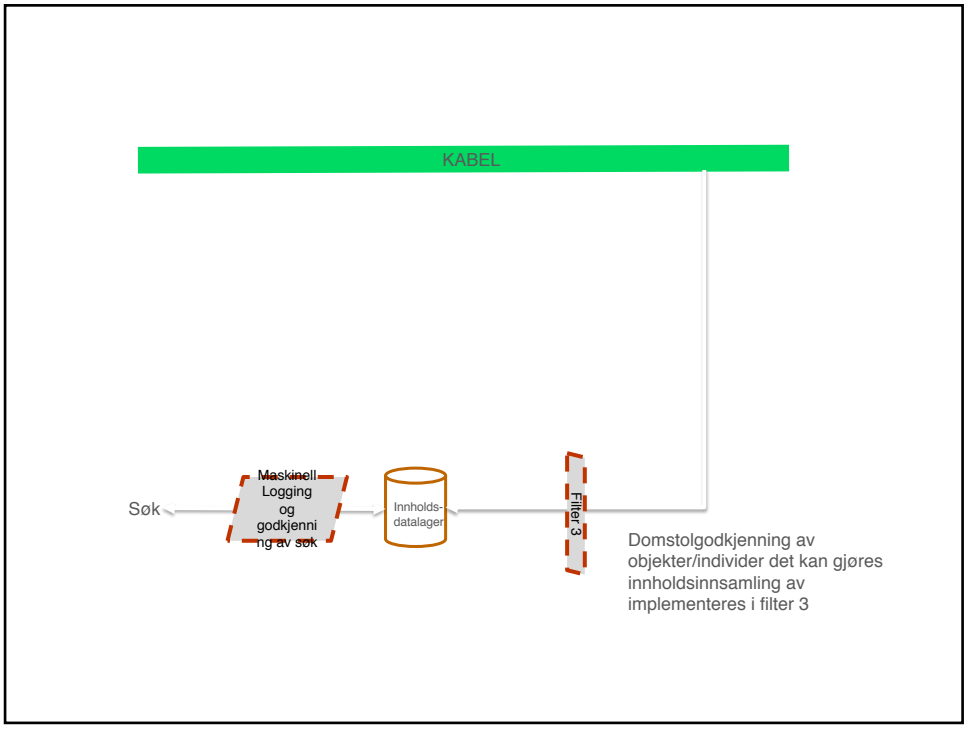
To some degree supported if “Legally acceptable”.

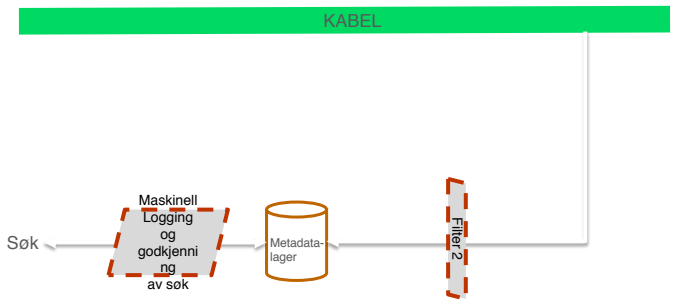
Transparency as a source of trust is not available.

Personnell with security clearance who inspects the installation for LI on our behalf.

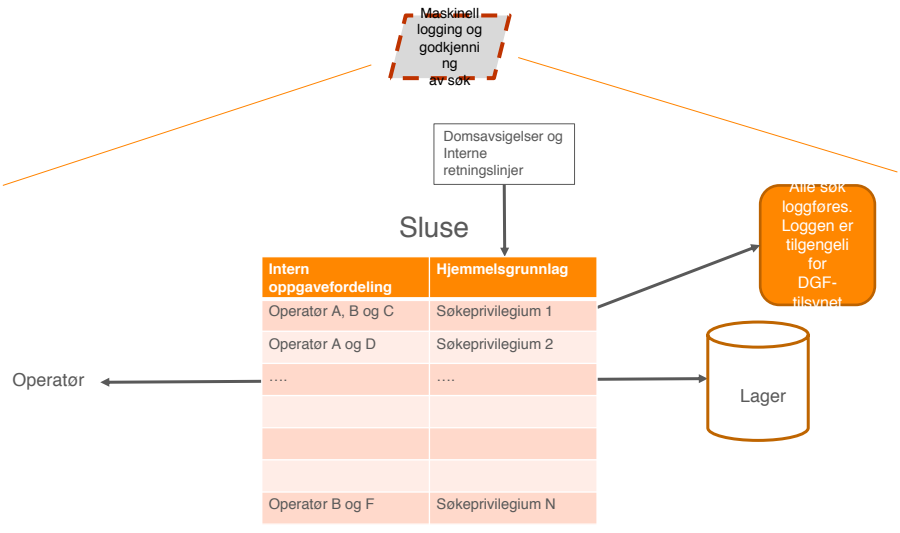


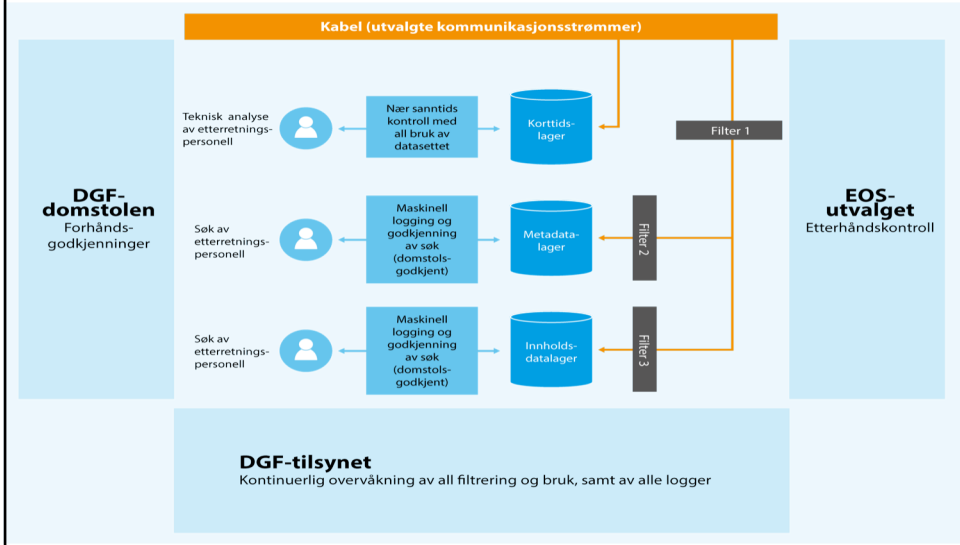

Funksjon for forhåndsgodkjenninge r
Uavhengig domstol
Funksjon for kontinuerlig overvåkning av bruken av DGF-systemet
DGF-tilsyn
Funksjon for etterkontroll av bruken av DGF-systemet
EOS-utvalg


KABEL
Søk
Maskinell Logging og godkjenni ng av søk
Innholds-datalager
Filter 3
Domstolgodkjenning av objekter/individer det kan gjøres innholdsinnsamling av implementeres i filter 3



Domstolgodkjenning av hvilke typer
søk som kan gjøres. Godkjenningene er basert på E-loven,
og identifiserer konkrete
Individer/objekter, eller konkrete handlingsmønstre.
Dette implementeres som tekniske søkesperrer, og overvåkes
av DGF-tilsynet.





Does Lawful Interception break the European Declaration of Human Rights?

Few countries can control their own digital vulnerability - most inherit vulnerabilities from other countries.

Digital vulnerability and national autonomy

- Small countries are completely dependent on international providers of digital equipment.
- We are to some extent governed - not only influenced - by decisions taken outside of our borders.
- Popular trends and products can undermine national autonomy.

What can a small country do when we have to buy equipment from abroad for our critical infrastructure?

- Countries like USA, Australia and India have banned Huawei/ZTE from critical parts of its infrastructure
- UK have set up a center that investigates Huawei's equipment
  - "Any risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated,"
- Many countries have worries, but have not taken legal action

Trust, but verify!

How do you verify electronic equipment?

State of the art

Much work done on how vendors and users of equpiment can collaborate to defend against third parties

Almost no available literature on cases where the vendor is the party you do not trust.

Structure of the problem

Scenarioes

1. **Vendor is malicious already at the time of delivery.**
2. **Vendor becomes malicious at a later stage.**

Consequences

1. **Espionage and surveillance**
2. **Render the equipment useless (or threaten to)**

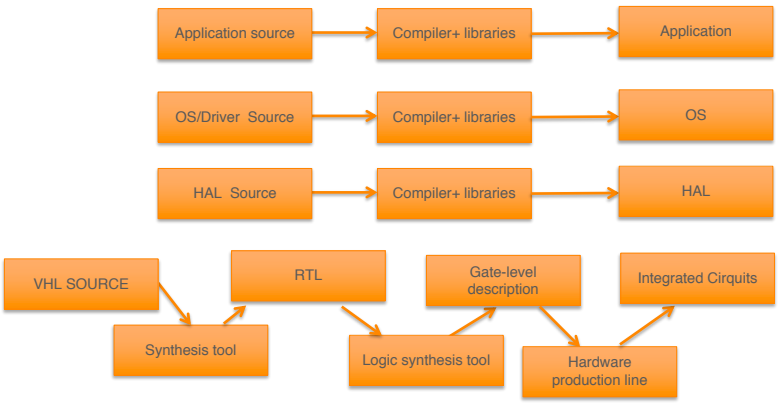
Questions

Can we detect preparations for a malicious act?

Can we detect that the act is taking place?

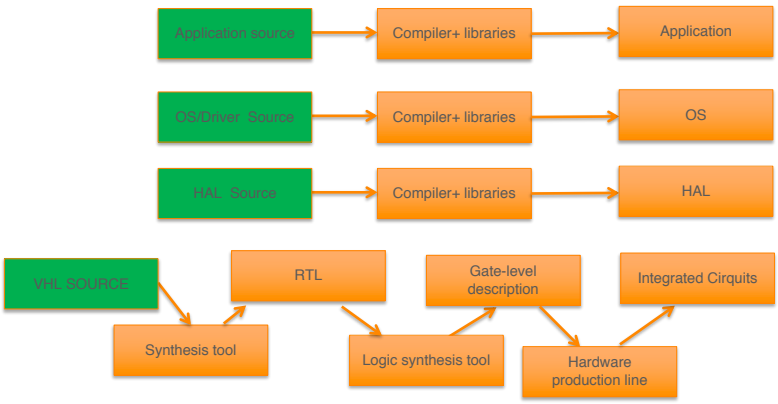
How many people need to be involved?

What is electronic equipment?



1. K.Thompson: Reflections on Trusting Trust, *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763
2. Huawei offers access to source code and equipment. http://www.bbc.co.uk/news/business-20053511.

Where can backdoors be introduced?



1. K.Thompson: Reflections on Trusting Trust, *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763
2. Huawei offers access to source code and equipment. http://www.bbc.co.uk/news/business-20053511.

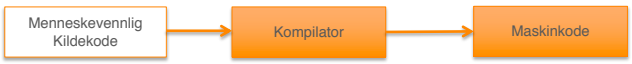
Yes, but at what points may a backdoor get introduced?

```
public class Test {

  public static void main(String args[]) {
    int x = 10;

    while( x < 20 ) {
      System.out.print("value of x : " + x );
      x++;
      System.out.print("\n");
    }
  }
}
```


```
01110011 01100101 01110010 01
01100101 01110010 00100000 01
01101000 01100001 01110100 00
01100100 01101001 01110011 01
01110010 01101001 01100010 01
01110100 01100101 01110011 00
01100001 01101110 01111001 00
01101001 01101110 01100011 01
01101101 01101001 01101110 01
00100000 01101101 01100101 01
01110011 01100001 01100111 01
01110011 00100000 01110100 01
00100000 01100001 01101100 01
00001101 00001010 00100000 00
```

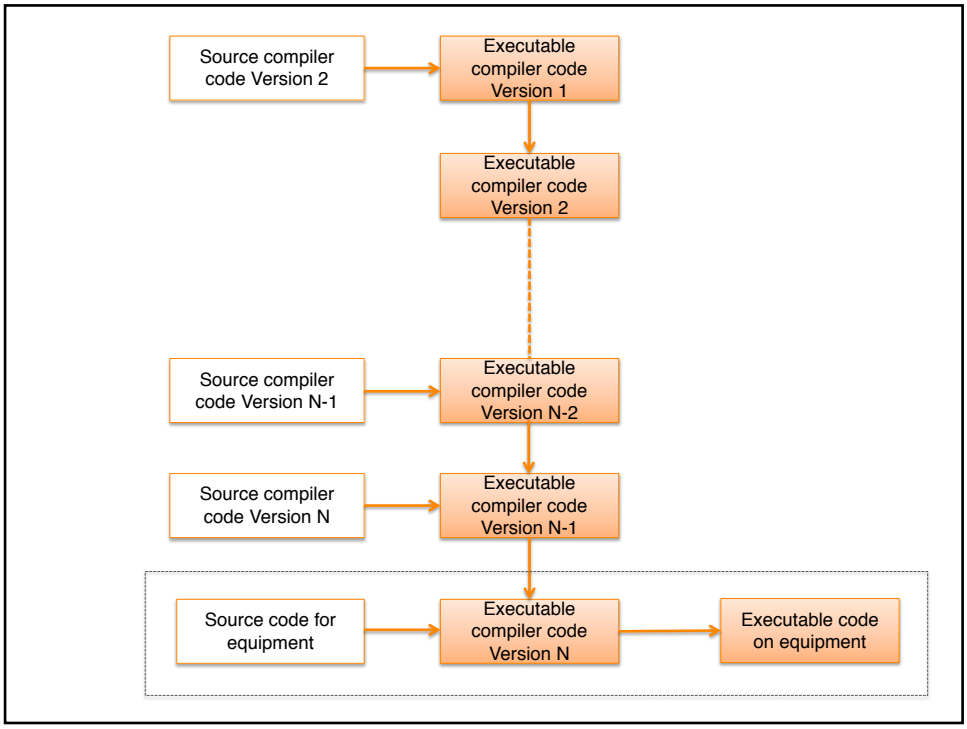
1. K.Thompson: Reflections on Trusting Trust, *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763
2. Huawei offers access to source code and equipment. http://www.bbc.co.uk/news/business-20053511.

I hvilket punkt i utviklingsprosessen kan en utstyrsleverandør plassere inn en bakdør?

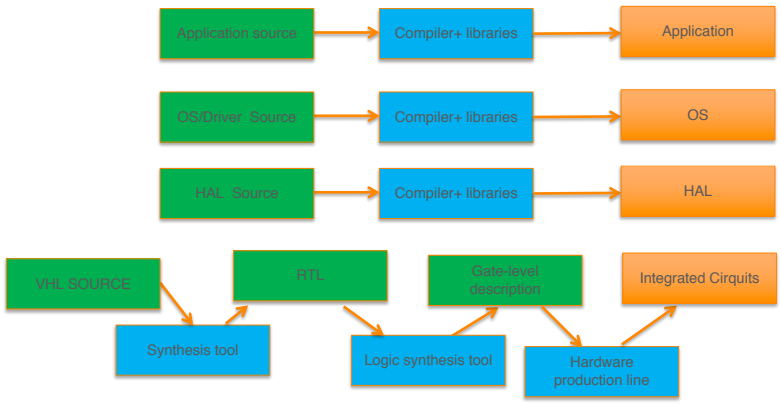


- Fravær av ondsinnede elementer i software – kildekoden er ingen indikasjon på at ondsinnede elementer ikke finnes i den koden som eksekveres.
- Fravær av ondsinnede elementer i hardware-beskrivelsen i et produkt er ingen indikasjon på at ondsinnede elementer ikke finnes i den ferdige chipen.
- Utviklingsteamet hos produsenten trenger ikke å være klar over at ondsinnede elementer legges inn i produktet.

1. K.Thompson: Reflections on Trusting Trust, *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763
2. Huawei offers access to source code and equipment. http://www.bbc.co.uk/news/business-20053511.



Where can backdoors be introduced?



1. K.Thompson: Reflections on Trusting Trust, *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763
2. Huawei offers access to source code and equipment. http://www.bbc.co.uk/news/business-20053511.

The questions

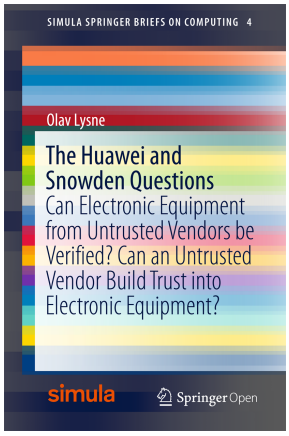
- Is the problem decidable in the Church/Turing sense?
- Can software quality management help us (models management, metrics, standards)?
- Can existing malware detection techniques help us?
- Can decompilation and reverse engineering help?
- How does the war between code obfuscation and de-obfuscation look?
- Can Formal Methods help?
- Dynamic methods/sandboxing?
- Can we contain untrusted modules architecturally?

These are the facts:

When an unknown third party is the enemy, there are methods that when correctly implemented and professionally applied makes it hard and resource demanding to break into a system without being detected.

When the equipment vendor is the enemy, there seems not to exist any method, even when professionally applied, that has significant effect on our abilities to deter or detect malicious acts.

Heterogeneity in the infrastructure and strong encryption end-to-end stand out as the only way forward.


SIMULA SPRINGER BRIEFS ON COMPUTING 4
Olav Lysne
The Huawei and Snowden Questions
Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?
simula
SpringerOpen


NOU
Norges offentlige utredninger 2015: 13
Digital sårbarhet – sikkert samfunn
Beskytte enkeltmennesker og samfunn i en digitalisert verden


Digitalt grenseforsvar (DGF)
Lysne II-utvalget