Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

PETweb – Privacy Enhancing Technology

for large scale web based services

VERDIKT Program Conference

Åsmund Skomedal

Norsk Regnesentral

Hell, Norway
29. october 2008

Overview

- Background
- Protective measures
- Privacy Principals
- Architecture
- Privacy Ontology
- Privacy Threat Impact Analysis
- Summary

Background

- Cost of storage approaches zero – can save everything
- Find out what end-users actually do to handle their privacy
- Find out what systems do
  - Portal owners, System integrators, Technology providers

Goals

- Develop tools to analyse the impact of privacy violations
- Identify efficient PETs in large scale web solutions
- Use a Case Study:
  MinSide/MyPage – the G2C portal
- Main partners: NR, HiG, Software Innovation, Sun, norge.no

Summary of protective measures (1)

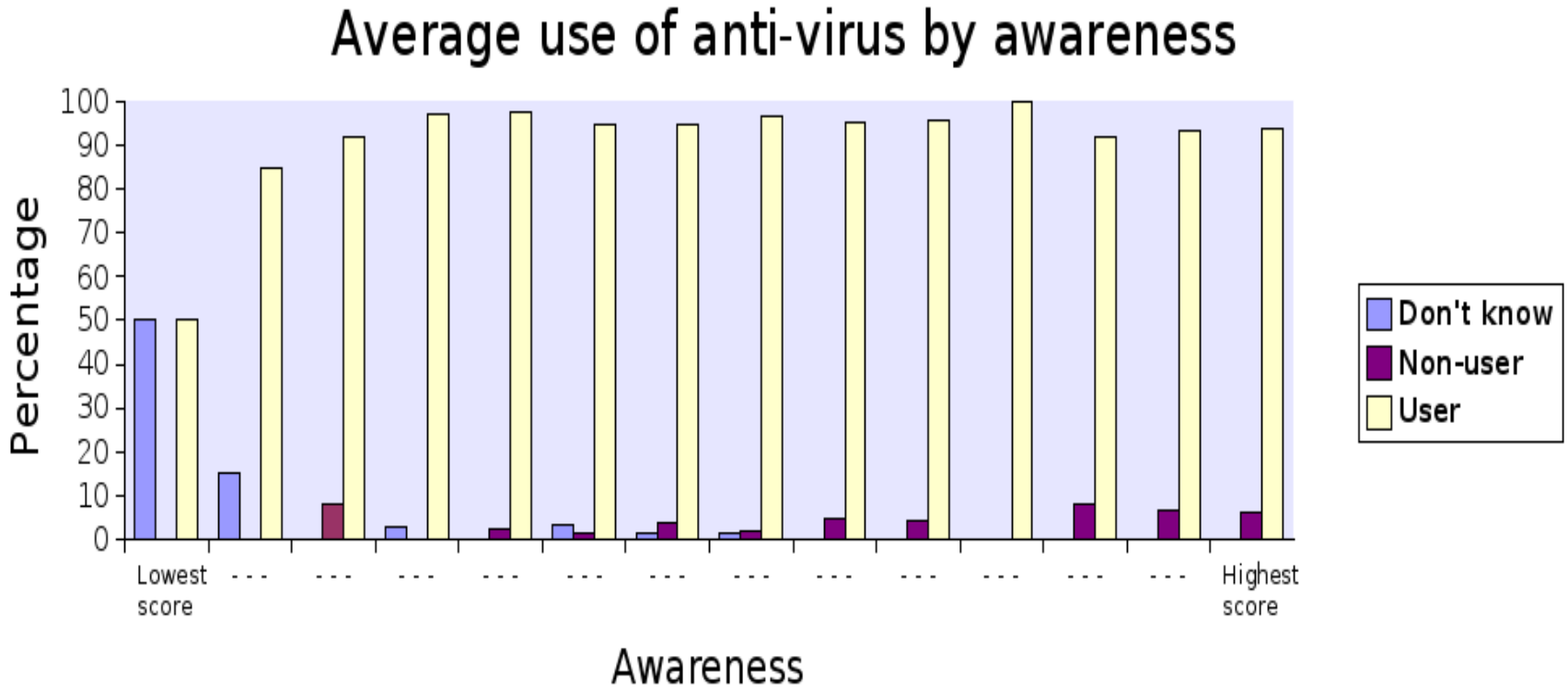
Findings from MSc Thesis (Høgskolen i Gjøvik) [F. Andreassen]

- There is a strong correlation between actual use and awareness
- Almost everyone knows about Viruses and the need to protect against it
- ca 70 % use Firewalls and pop-up blockers
- ca 50% use anti spyware SW on average

Why is this a problem?

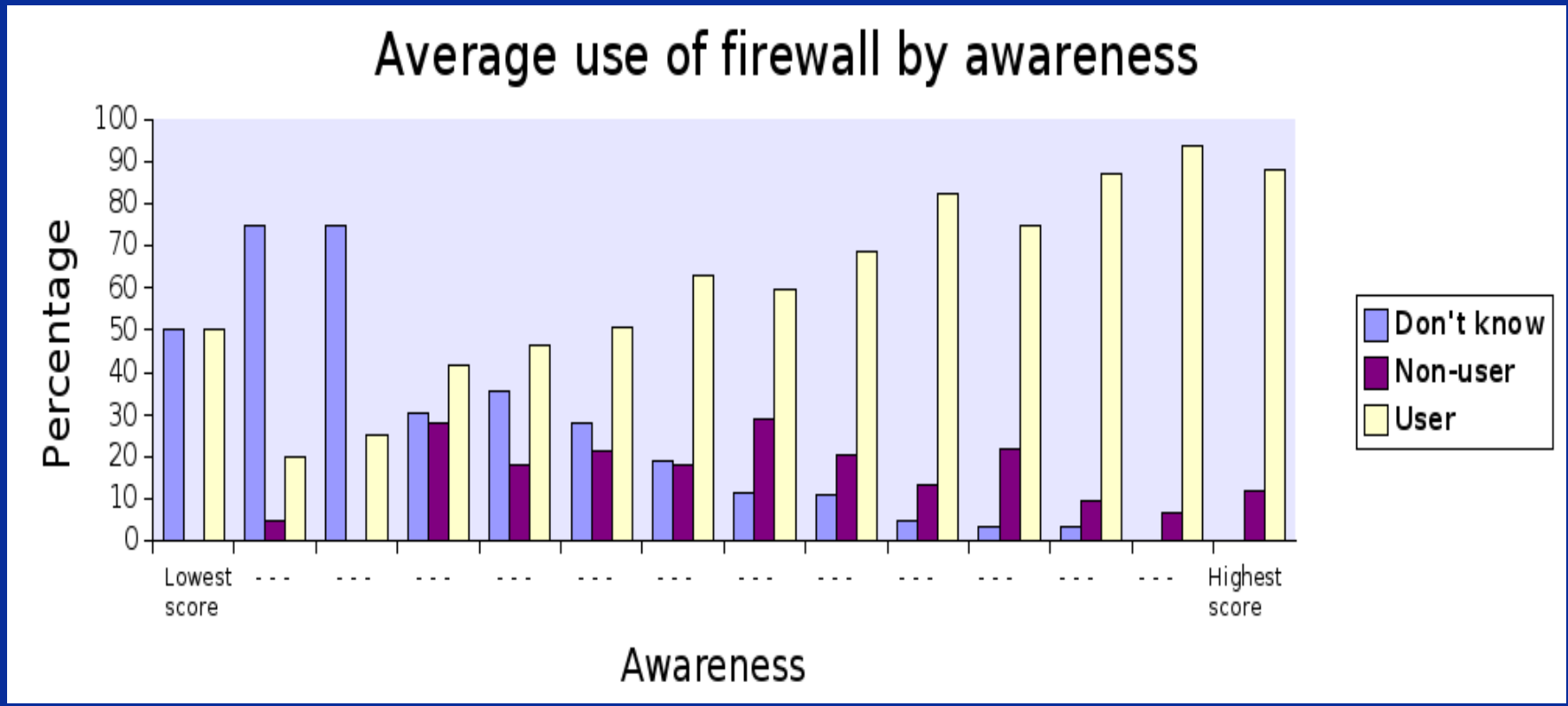
In the second quarter of 2006, close to x% of checked U.S. home computers contained forms of spyware.

Who uses Anti Virus (AV) SW



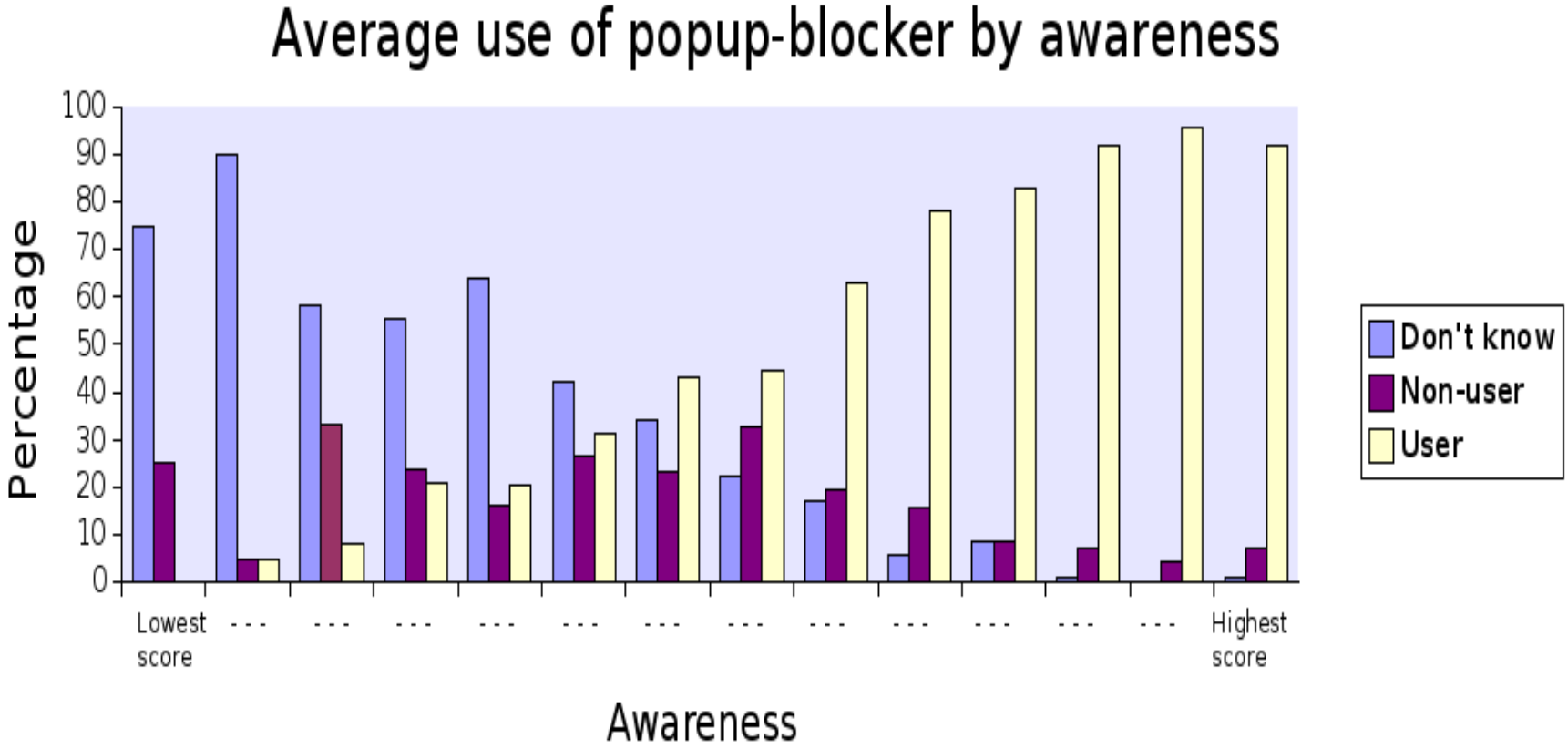
- In total: 92.1% uses AS SW -> OK !

Who uses Firewalls (FW)



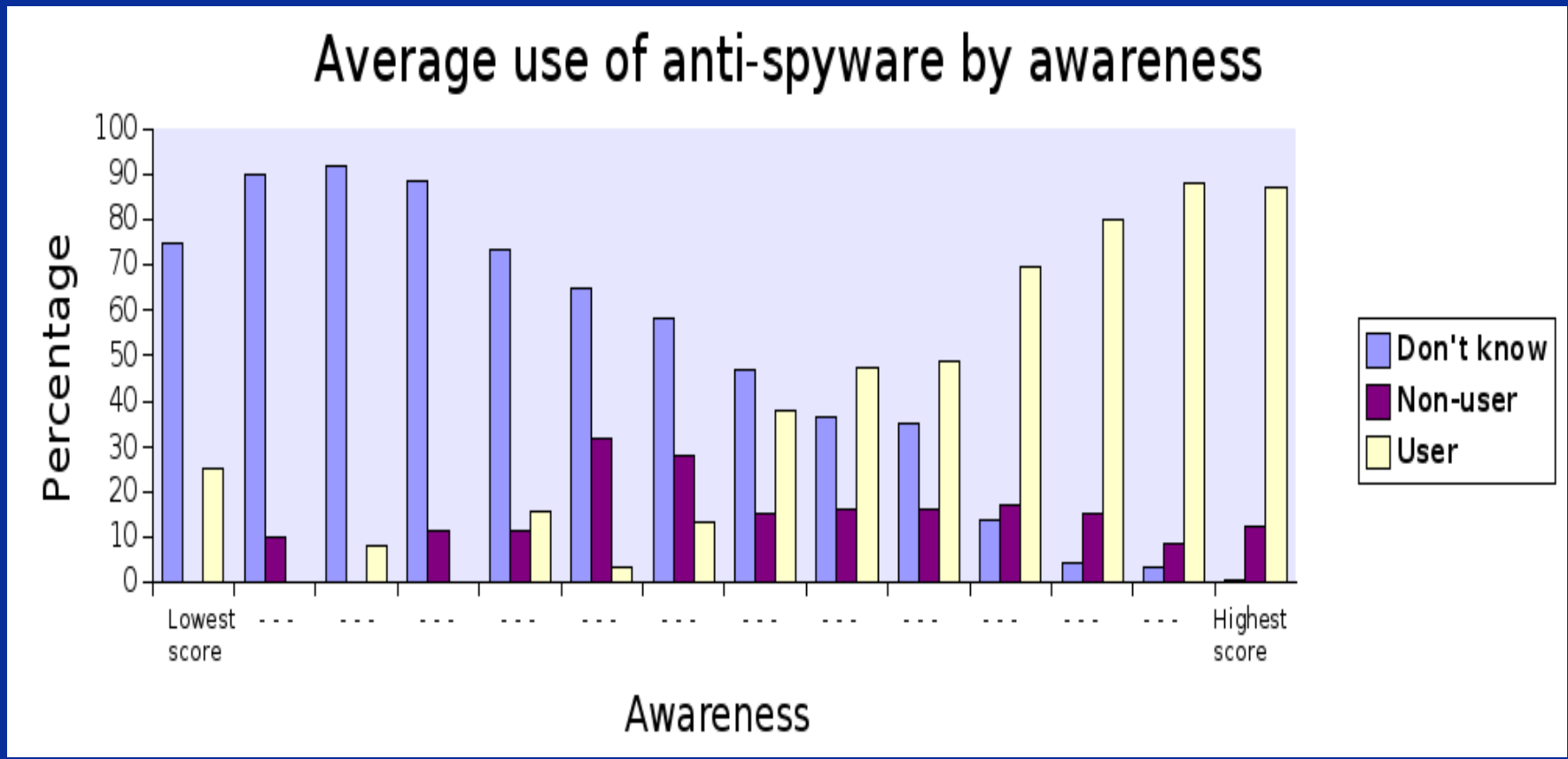
- In total: 72% uses a FW -> OK !

Who uses Pop-Up Blockers



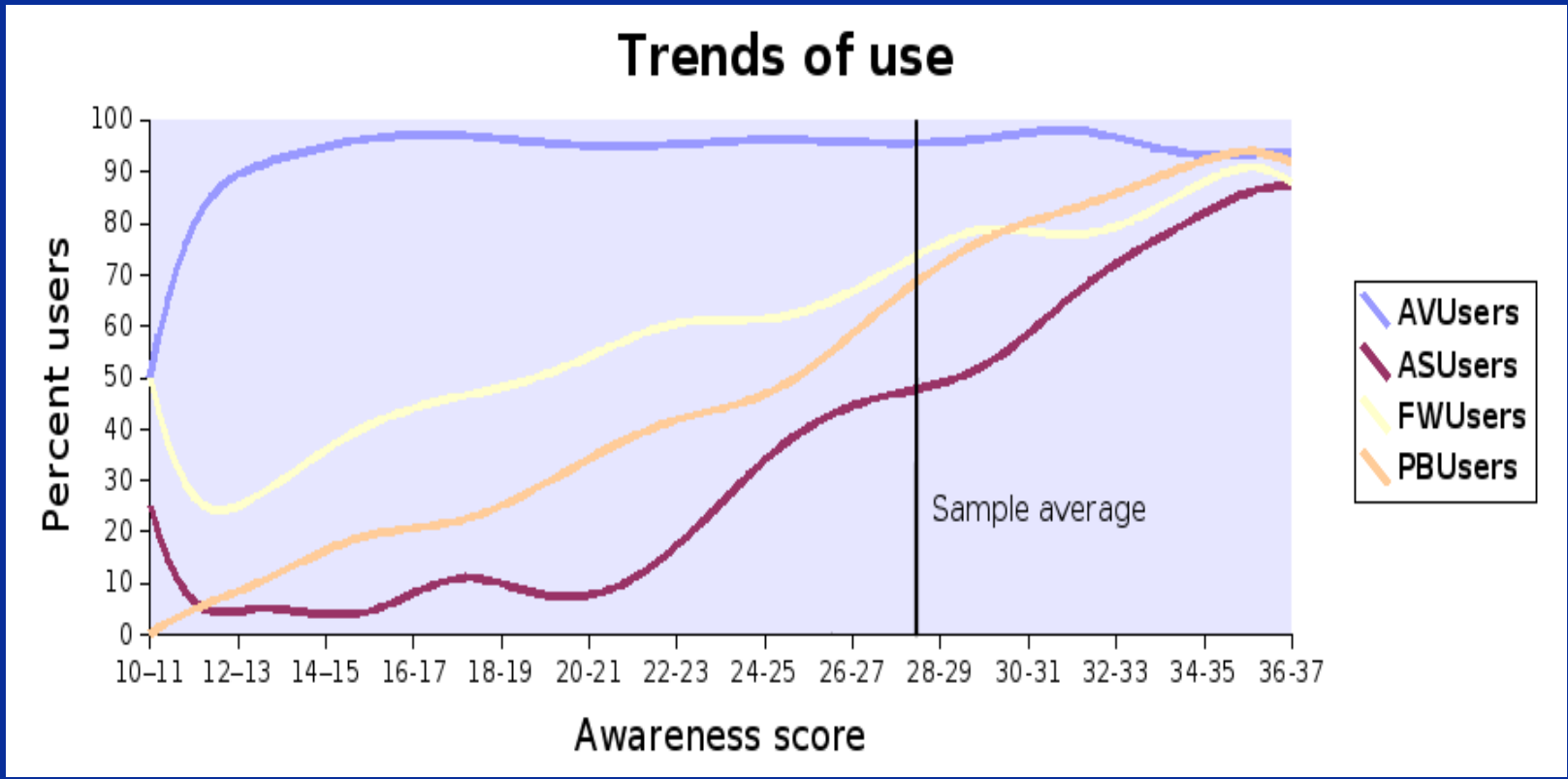
- In total: 66 % uses AS SW -> fair !

Who uses Anti Spyware (AS) SW



- In total: 52 % uses AS SW and 23% don't know !

Summary of protective measures (2)



In the second quarter of 2006, close to 90% of checked U.S. home computers contained forms of spyware.

Best guess
⇒ many get spyware without knowing about the threat
⇒ even more get it with Anti Spyware installed
When citizens use PCs to access SENSITIVE private information this is an issue

Privacy Principals – basis

1. Principles concerning the fundamental design of products and applications:
   - Data minimization (maximum anonymity and early erasure of data)
   - Transparency of processing
   - Security
2. Principles concerning the lawfulness of processing:
   - Legality (e.g. consent)
   - Special categories of personal data
   - Finality and purpose limitation
   - Data quality
3. Rights of the data subject:
   - Information requirements
   - Access, correction, erasure, blocking
   - Objection to processing
4. Data traffic with third countries

Privacy Principals – basis

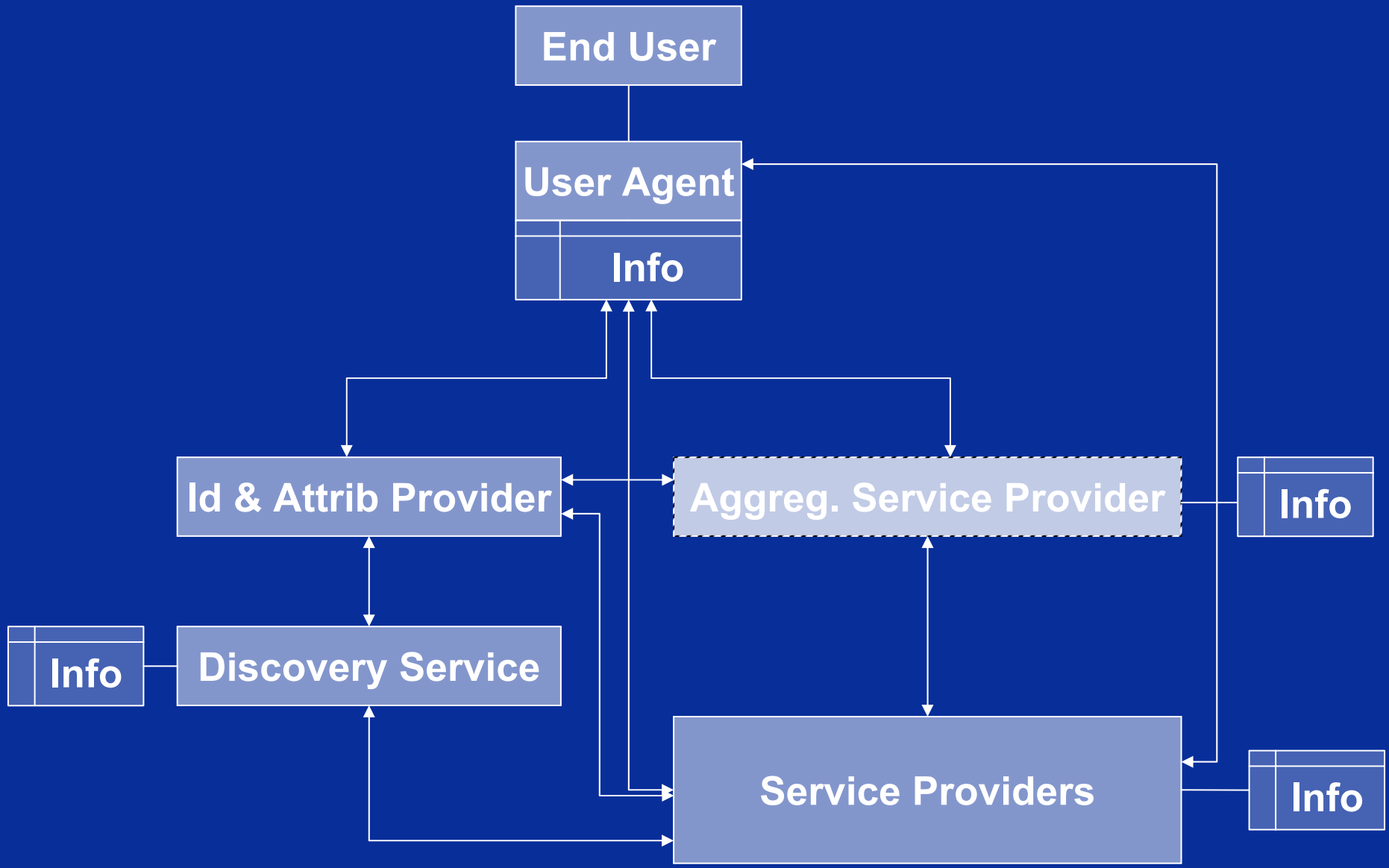
5. Notification requirements
6. Processing by a processor – responsibility and control
7. Other specific requirements resulting from the
   - Directive on Privacy and Electronic Communications 2002/58/EC/,
   - Data Retention Directive 2006/24/EC and
   - the Norwegian legislation.

The grouping of privacy facilitation principles of data processing have been used by the ICPP – the Data Protection Authority of Schleswig-Holstein, Germany for the purposes of conducting privacy audits, and in particular by the catalogue of requirements of the ICPP "Privacy Seal for IT Products"

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

The PETweb Architecture



Privacy Ontology

Privacy Objectives

- **Data protection** – fair information practices: anonymity, unlinkability, pseudonymity,
- **Unobservability**
- **Security**: Conf., Integrity, Accountability, Availab.

Threat Actor
- Intent
- Capabilities
- Opportunities

Automated
- Scripted
- Controlled
- Autonomous

Manual

v.nr.no

Threat Target

Threat

Threat Agent

1..* 0..* 0..* 1..*

Passive

Active

Security Privacy
- Interception
- Manipulation
- Repudiation
- Denial of Service

Information Privacy
- Collection
- Processing
- Dissemination
- Invasions
- Non-compliance

as applicable
- roles (outsider, system admin, foreign, intelligent, etc)
- observing / interfering upon agreed rules

Locality threats
- global attackers (Governments)
- local attacker (Local admin)

User threats
(sender, receiver)
- hostile user
- user errors
- user's misuse
- user abuses

Admin threats
- errors of commiss.
- errors of omission
- hostility (data, user)
- violation of user privacy policy

Developer threats
- SW containing security flaws
- input validation, integer/buffer overflows

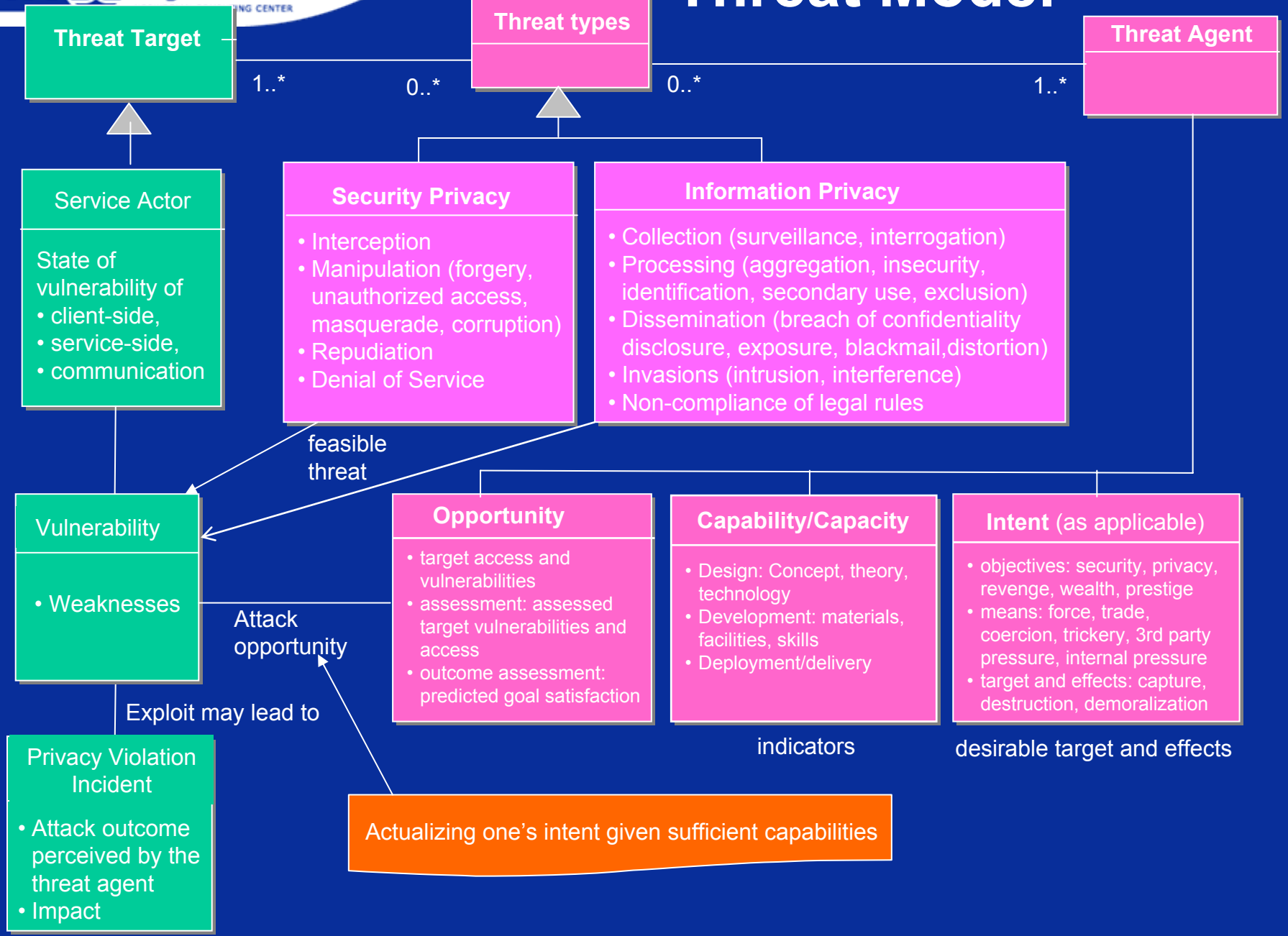
System threats
- component fails
- degradation over time
- excess voltage

Hackers threats
- spoofing
- social engineering
- malicious code exploitation
- eavesdropping

Threat Model

Norsk Regnesentral

www.nr.no



Privacy Threat Impact Analysis

- Privacy ≠ Security
- Model needs to capture
  - Capability, Intent and Opportunity
  - Assets, actors and threats
  - "Impact"
- Goals:
  - Find the weak spots -> efficient PETs
  - Understand how Data Subjects and Data Processors view the same threat differently
  - What assumptions can Service providers make on behalf of end users and their protective measures

Privacy Threat Impact Analysis tool

For each … calculate

- Asset
  - Threat Types (Locality, User, Developer … Hacker)
    - Threat Agent
      Properties
      - Auto/Manual, Active/Passive
      - Intent, Capability, Opportunity

        - Threat 1, Impact
        - …
        - Threat n, Impact

Min Side (norge.no)

MinSide is an Aggregated Service Provider

- Uses “existing” authentication methods
- Min ID is Identity Provider (based on SAML), federation is Possible

Unconfirmed estimates

- Federation is not anonymous when it can be ?
- Personal Information transferred (and stored) in the User PC is not protected by Min Side – and not by the average user ?

Some open issues

- Availability vs Privacy
  - What is the responsibility of the (Aggreg.) Service Provider knowing that end-user security is more or less inadequate
  - Should MinSide place Security requirements (SW !?) on the User PC
  - What about on-line security evaluations
- User volume vs Security
  - What are adequate Authentication Methods to access SENSITIVE private information

PETweb summary

Background

- Awareness study => many users without adequate security

PETweb Framework consists of

- System Architecture
- Ontology
- Privacy Threat Model
- Privacy Impact Analysis tool

Validation of results with Min Side

- Validate the PETweb framework and tools
- Point out weak spots => identify efficient PETs
- Identify Open Issues
  often a trade-off between Data Owner and Data Processor interests