Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

PETweb – Privacy Enhancing Technology

User Awareness and current use of protective measures

Background and Open issues

Åsmund Skomedal

Norsk Regnesentral

Oslo, Norway

11. December 2007

Overview

- Background
- Awareness and Protection
- PETweb Architecture
- Roles & motivation
- An Hypothesis
- Some Relevant Questions (and answers)
- Summary

Privacy & Security in the news …

Morgenvold

ID-tyver stjal Jan Fredrik Karlsens nummer og forandret adressen. Dommeren fulgte sporet til den skyldige kassen.

Tyver er Idol-Karl hjemmeadr

Godt forberedt

Aftenposten

Onsdag 14. november 2007. Uke 46. Nr. 529. 148. årg. Kr. 15. Fly/ekspress: Nord-Norge kr. 20.

Gi en gave som mottageren selv kan bestemme inneholdet i
UNIVERSAL Presentkort
www.presentkort.no

Jeg glemmer å se de små tingene som gjør hverdagen unik. De små tingene som gjør meg lykkelig.
Si ;D
KULTUR • side 27

REISE

Vanlig lugar ikke bra nok
KULTUR • side 16 og 17

Persondata ligger åpent

Ut på nett. Slurv med sensitive data er utbredt i kommunene. Fødselsnumre, skolefravær og jobbsøknader er blitt lagt ut i søkbar form på nettet.

Ålesund. Datatilsynet gransket i vinter rutinene i Ålesund, hvor navnene på en rekke sosialklienter var gjort lett tilgjengelig gjennom vanlige nettsøk. DEL 1 • side 10 og 11

BORGERLIG DANSK SEIER

Opptellingen etter Folketingsvalget tydet i natt på at statsminister Anders Fogh Rasmussen får fortsette

SKJERPET KONFLIKT I PAKISTAN

Background for PETweb

- 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 Norwegian G2C portal
- Main partners: NR, HiG, Software Innovation, Sun, norge.no

Awareness and Protection (1)

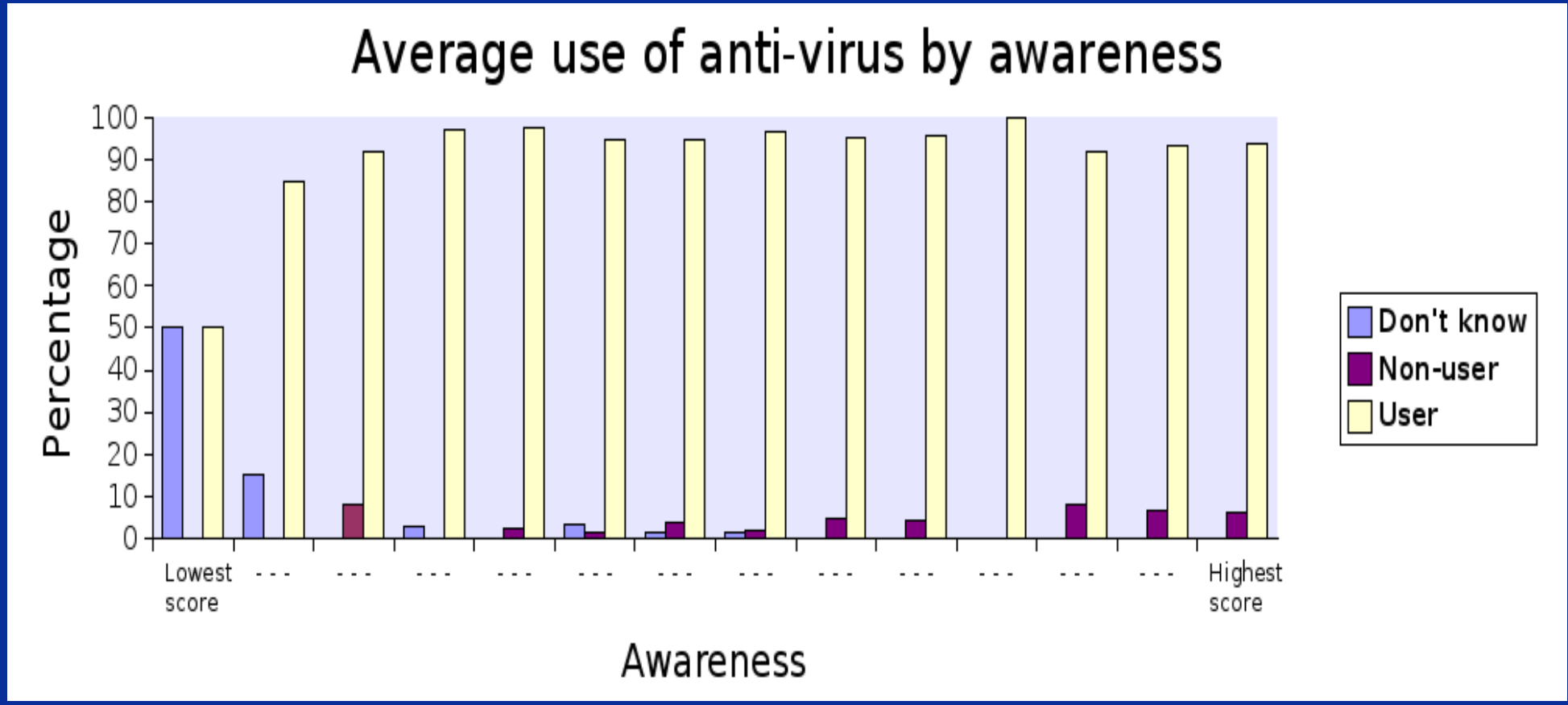
Findings from MSc Thesis (Høgskolen i Gjøvik)

- There is a strong correlation between awareness and actual use of protective measures
- 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?

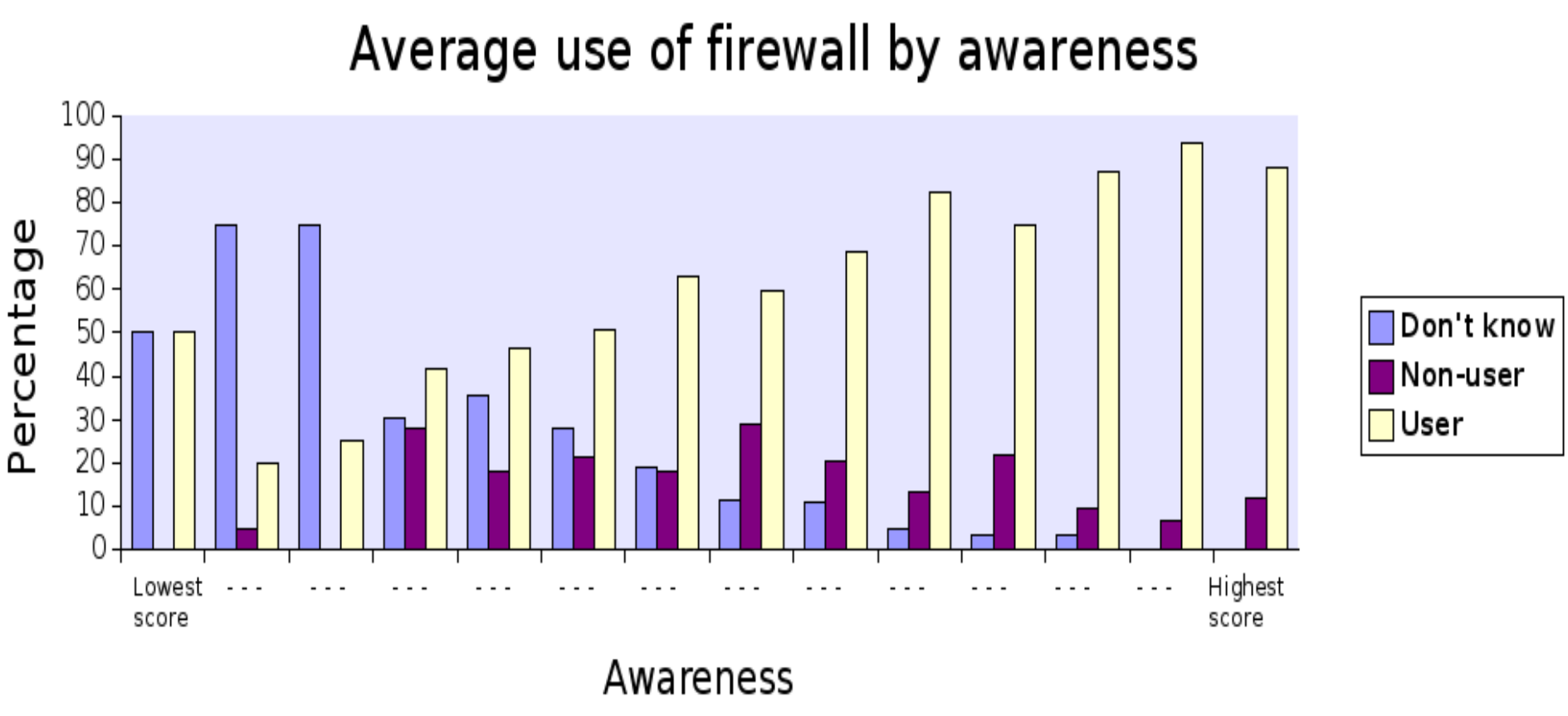
In the second quarter of 2006, close to x% of checked U.S. home computers contained forms of spyware.

Who uses Anti Virus (AV) SW



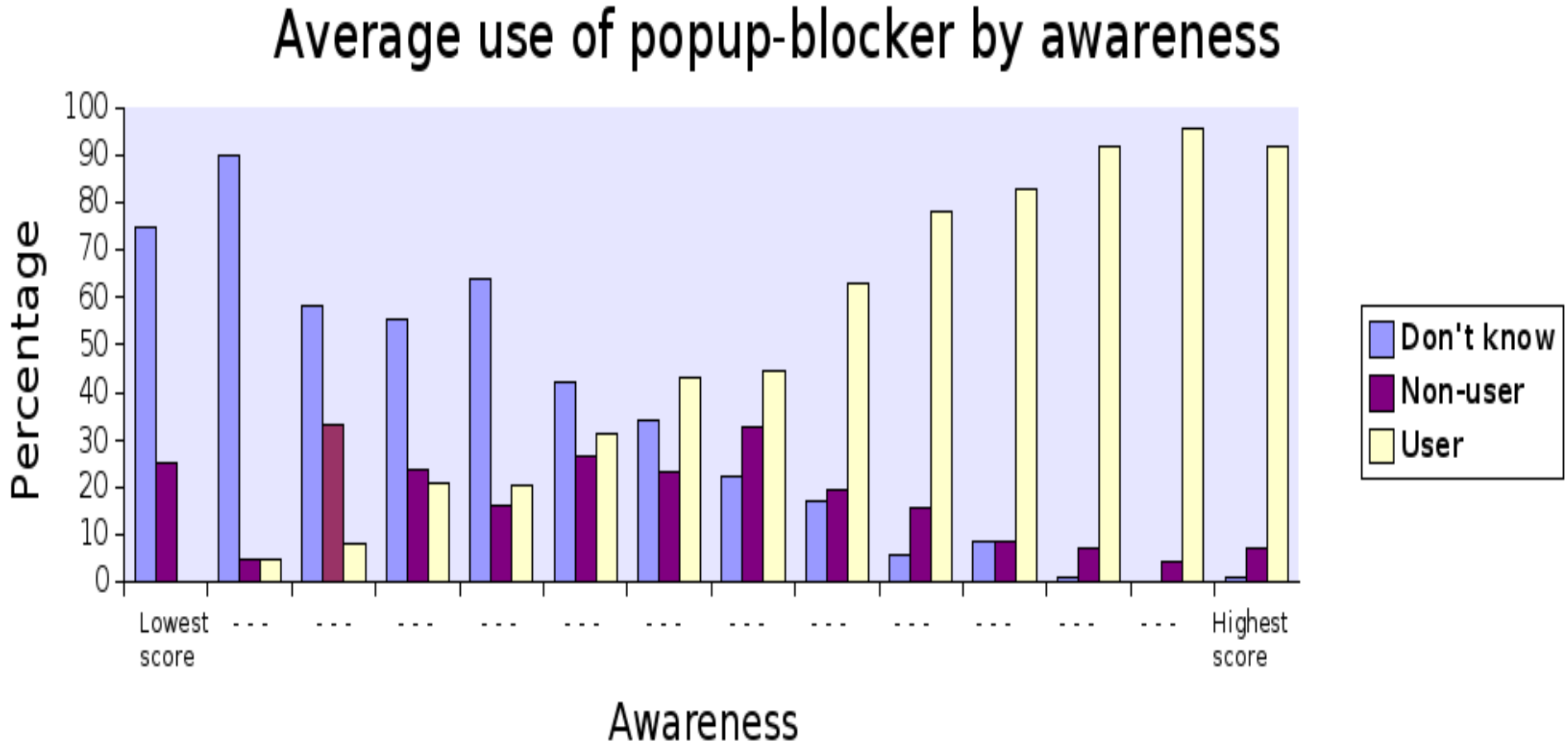
- **In total: 92.1% uses AS SW -> OK !**

Who uses Firewalls (FW)



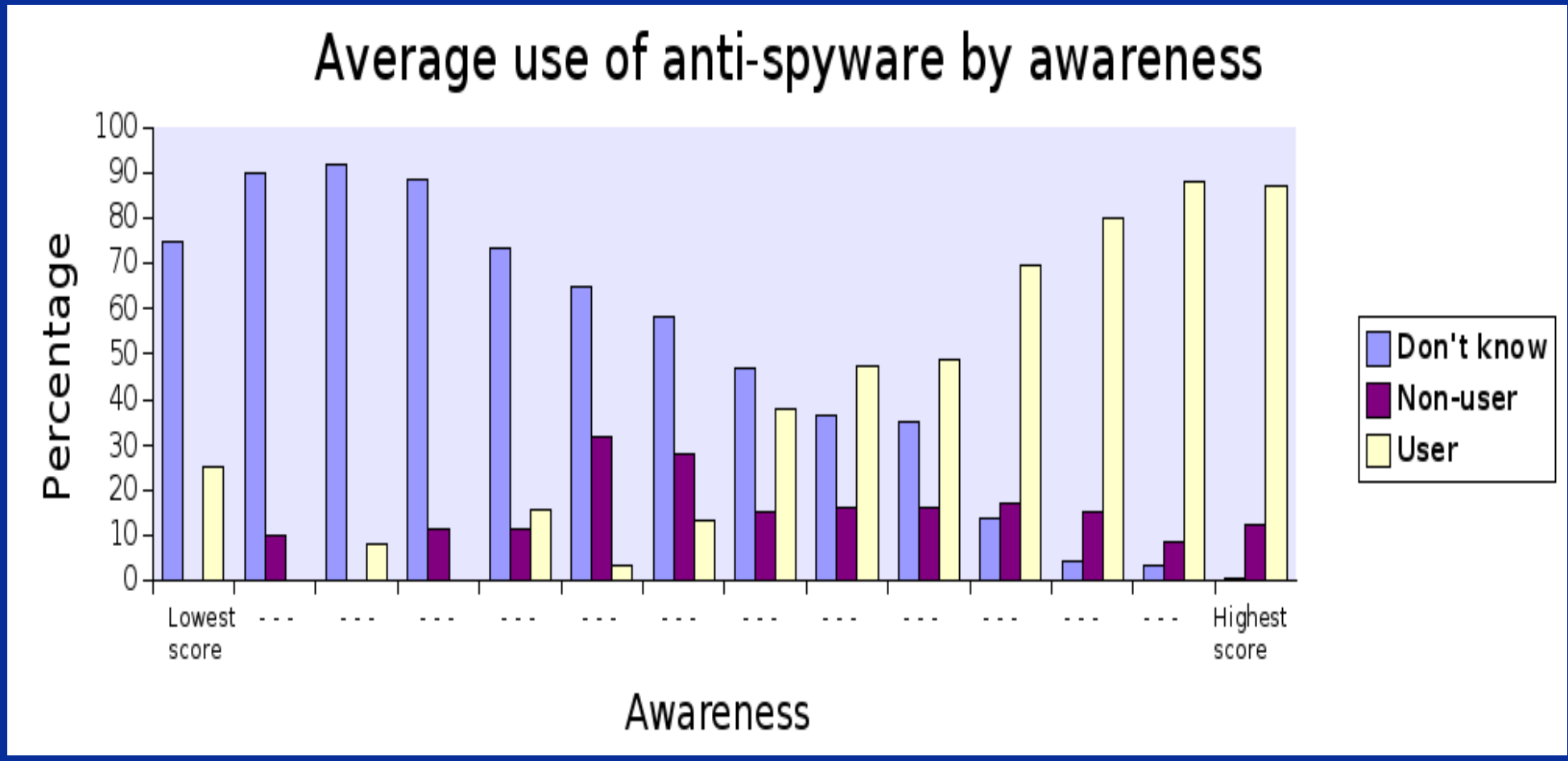
- In total: 72% uses a FW -> OK !

Who uses Pop-Up Blockers



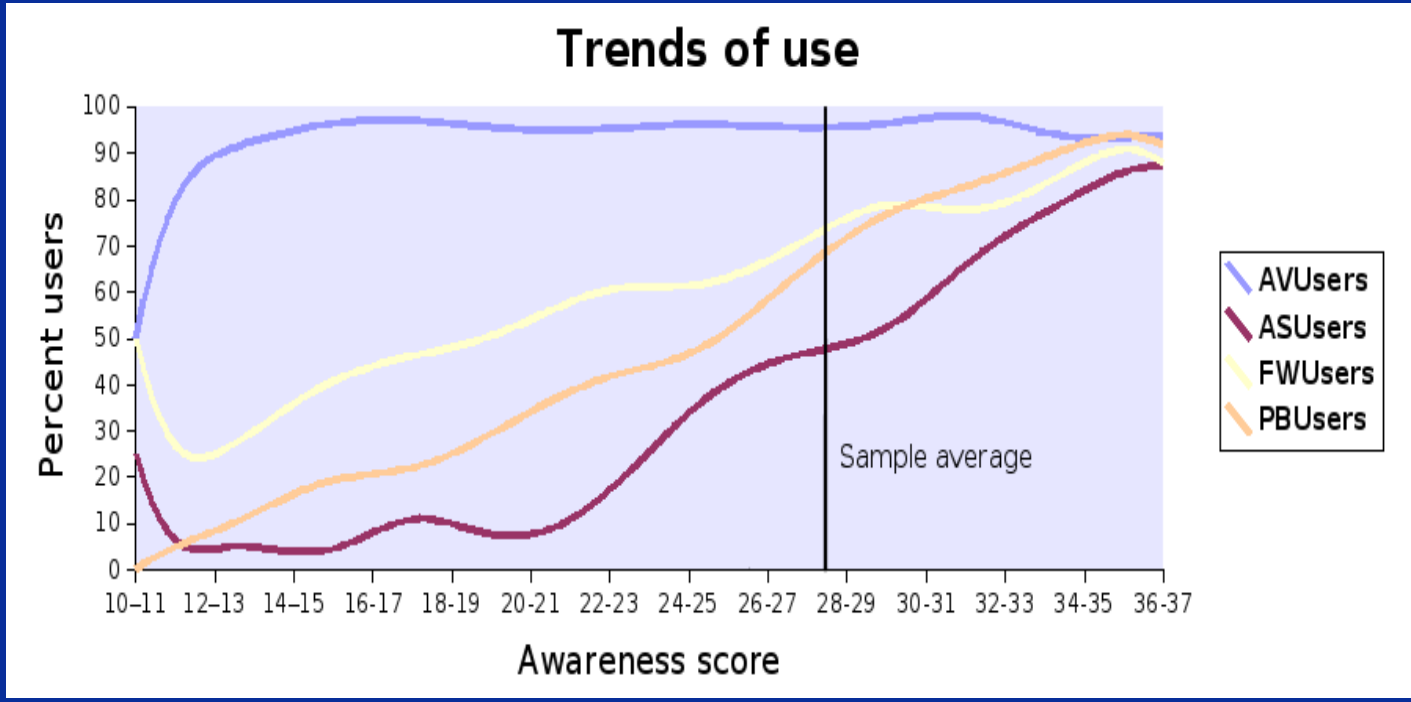
- **In total: 66 % uses AS SW -> fair !**

Who uses Anti Spyware (AS) SW



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

Awareness and Protection (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

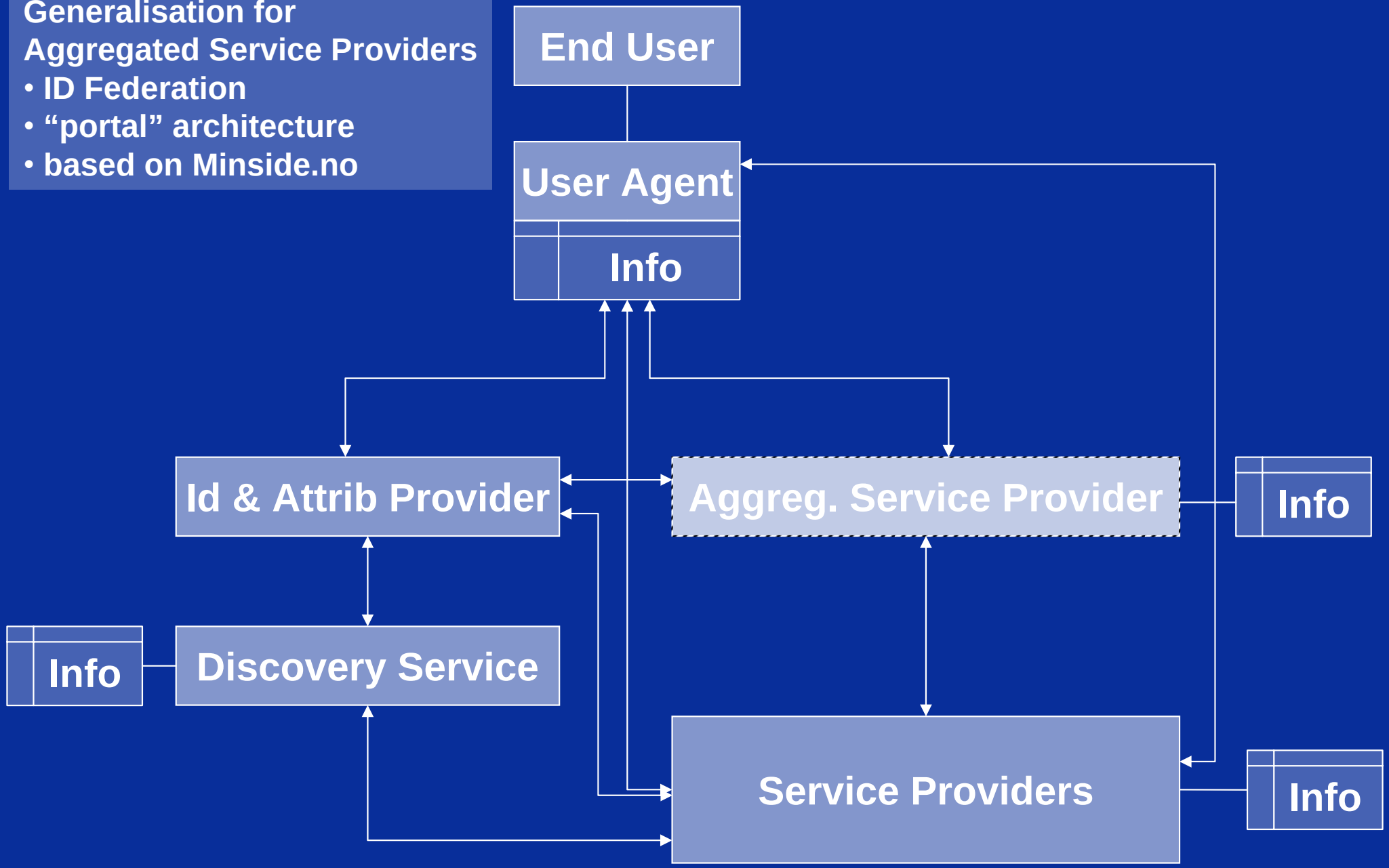
When citizens use PCs to access SENSITIVE private information this is an issue !!

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

The PETweb Architecture

Generalisation for Aggregated Service Providers
- ID Federation
- “portal” architecture
- based on Minside.no



Roles & motivation

Entity	Scope	Privacy Awareness	Security Awareness	Counter measures
End User	Just one person	Low to high	Medium to high	Variable
User Agent	One or few			
Service Provider	ORGANISATION	Medium ?	Medium ?	Fair
Aggregated Service Prov	CENTRALISED ORGANISATION	Medium	Medium ?	Fair
ID & Attrib Provider	CENTRALISED ORGANISATION	Medium	High	Good
Discovery Service	CENTRALISED ORGANISATION	Medium	High ?	Fair

Evaluation of roles, awareness and estimated countermeasures:

- **Users will start at the lower end of the awareness score and move upward with experience => learn by experience**
- **Organisations potentially have external motivation (legal, reputation, …) that improves awareness before and thus countermeasures BEFORE introducing a new service**

The Privacy Threat Impact Analysis will elaborate this …

An hypothesis about End Users

Assuptions

- Users will start at the lower end of the awareness score and move upward with experience (unless they read up on current security issues BEFORE using a new service)
- There is a considerable time-lag from a new privacy (or security) threat appears until wide spread deployment of counter measures is in place at the User Agent

  => this is the “window of opportunity” where attack efficiency is high (and the average user is completely ignorant)

HYPOTHESIS

Customers have VERY varying security level on their Agents, AND
the flow of new threats will not end;

there will ALWAYS EXIST a large proportion of End Users that have INADEQUATE security measures

An interesting question is; can (A)SPs leave full responsibility for the risk implied by a service to the customers ???

Some relevant Questions

Some issues that need to be handled and CONSISTENT across all G2C services

- WHO shall perform the Privacy Impact Analysis for a G2C Service ?
- How is the risks associated with using a service communicated with the End Users?
- Who shall define appropriate authentication mechanisms for SENSITIVE Private Info?
- Who shall define what information is “SENSITIVE PRIVATE” and what is “PRIVATE” ?
- Who shall define the (legal and technical) responsibility of End users?
- How is the responsibility of End Users communicated with the User?

Who has the operational responsibility for

- deploying (& evaluating ?) User Agent countermeasures
- evaluating the Infrastructure [(A)SP, IDM] countermeasures
- for handling privacy breaches

Some possible Answers (1)

Some issues that need to handled

- WHO shall perform the Privacy Impact Analysis for a G2C Service ?
  - No one
  - The operator with the PETweb tool
  - QA and approval / involvement by Datatilsynet (?)
- How is the risks associated with using a service communicated with the End Users ?
  - web info
  - ASP offers on-line privacy and security tests for Clients
  - ASP offers guidelines / references to protective measures
  - ASP offer free protective measures
- Who shall define appropriate authentication mechanisms for SENSITIVE Private Info?
  - Not regulated – it is left up to the service provider (budget)
  - G2C follows the Standard; PKI i offentlig sektor (do they ?)
- Who shall define what information is “SENSITIVE PRIVATE” and what is “PRIVATE” ?
  - Each SP -> leaves up to the ASP to handle inconsistencies !
  - The G2C ASP, the Data Inspectorate, Br Reg, … an USO (Unidentified Stds Org.)
- Who shall define the (legal and technical) responsibility of End Users
  - the Service Provider , i.e. the operator (Ref. Bank ID …) ???
  - the National Data Inspectorate (Datatilsynet) ?
- How is the responsibility of End Users communicated with the User
  - by a Privacy Statement that has poor (?) readability ?
  - by a normalised Privacy and Security statement (the user MUST read)

Some possible Answers (2)

Who has the operational responsibility for ?

- **deploying (& evaluating ?) User Agent countermeasures**
  - **the End User without assistance**
  - **the End User with assistance from the (A)SP or ISP**
- **evaluating the Infrastructure [(A)SP, IDM] countermeasures**
  - **the service provider only**
  - **external evaluators, according to scheme xyz**
  - **the Norwegian Post & Telecom (NPT) Authority**
  - **the Norwegian Data Inspectorate**
- **for handling privacy breaches**
  - **the End User without assistance**
  - **the End User with assistance from the (A)SP or ISP**

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 Agent is not protected against Spyware by Min Side service offer ?

Some open issues

- Availability vs Privacy
  - Should MinSide place Security requirements (SW !?) on the User Agent, e.g. what about an internet café ?
  - What about on-line security evaluations ?
- User volume vs security
  - What are adequate Authentication Methods to access SENSITIVE private information? Std. for PKI in the Public sector => this is “PERSON HIGH” i.e. based on Qualified Certificates & Smart Cards

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

… end

Thank you for your attention !

Agenda 11 December 2007 - Oslo

- ”User Awareness and current use of protective measures”, by Dr. Åsmund Skomedal, Norsk Regnesentral
- “Privacy Principals and some business considerations”, by scientist Lothar Fritsch, Norsk Regnesentral
- ”Ontologi for personvern og trusler”, by senior scientist Dr. Habtamu Abie, Norsk Regnesentral
- ”The surveillance state and our protection by deploying PETs”, by Drs. John J. Borking, Director, Borking Consultancy, The Netherlands