Privacy Principles and Requirements

Bakgrunn, prinsipper og krav

PETs – Privacy Enhancing Technology

Hvordan ivareta sikkerheten for personinformasjon på nettsteder?

Åsmund Skomedal

Forskningssjef
Norsk Regnesentral

Oslo, 10. april 2008

Innhold

- Bakgrunn - POL (Loven …)
- Brukerkompetanse og beskyttelse
  - Brukerundersøkelse
  - En hypotese
- Personvernsprinsipper
- Personvernskrav til systemer
- PETweb metoder
- Verktøy
  - Privacy Impact Analysis
- Oppsummering

Privacy & Security in the news …

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

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

Morgenvold

ID-tyver stjal Jan Fredrik Karlsen nummer og forandret adressen

Tyver er Idol-Kar hjemmeac

Godt forberedt

Personopplysningsloven (POL)

- Formål og spesifikasjon
  - … beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.
  - Personvernsopplysninger: opplysninger og vurderinger som kan knyttes til en enkelt person
  - Samtykke: en frivillig, uttrykkelig og informert erklæring …

- Dette er en god og viktig lov ettersom det blir
  - stadig mer informasjon lagret om borgerne
  - stadig mer automatisk behandling basert på personopplysninger

- Tillit til behandlingsansvarlige er (overdrevent ?) stor

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

Awareness and Protection (1)

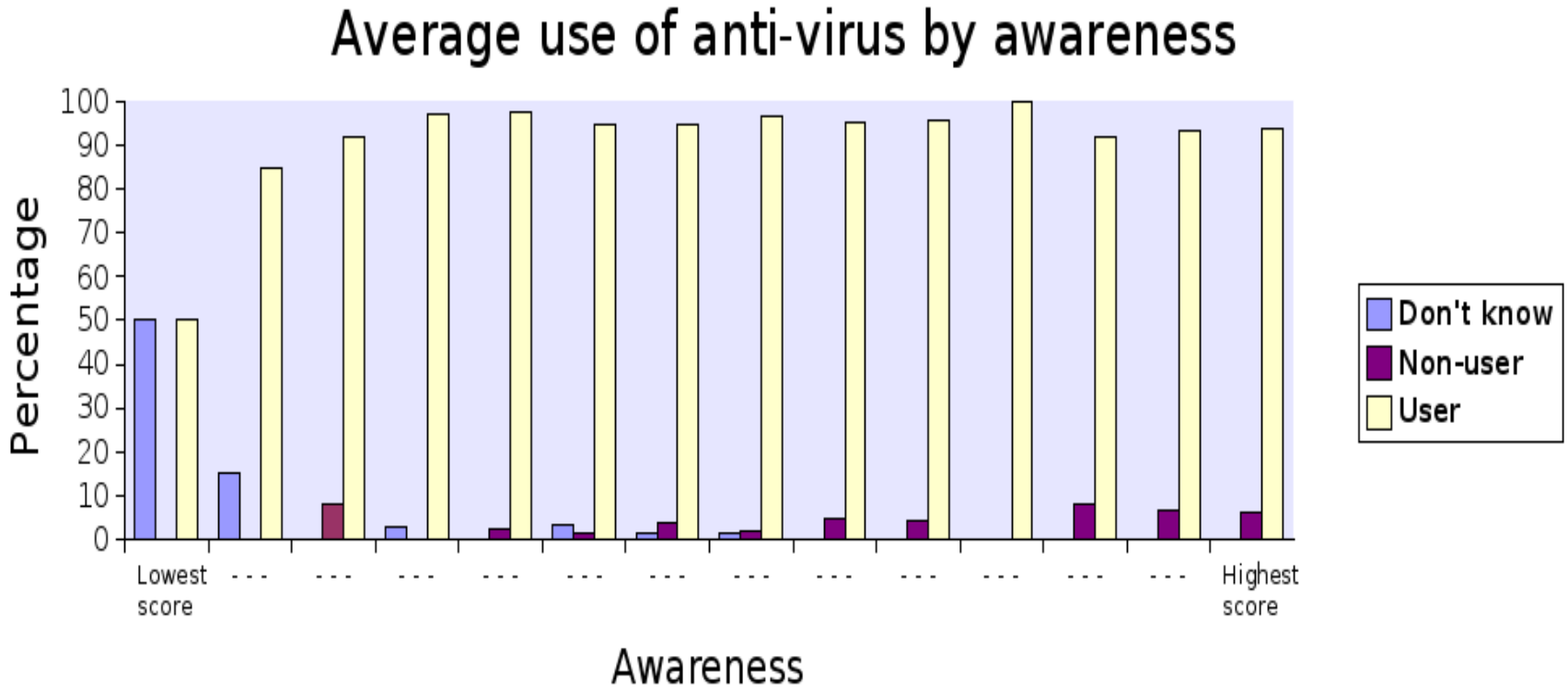
Findings from MSc Thesis of Freddy Andreassen (Høgskolen i Gjøvik, supervised by Prof. Einar Snekkenes)

- 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?

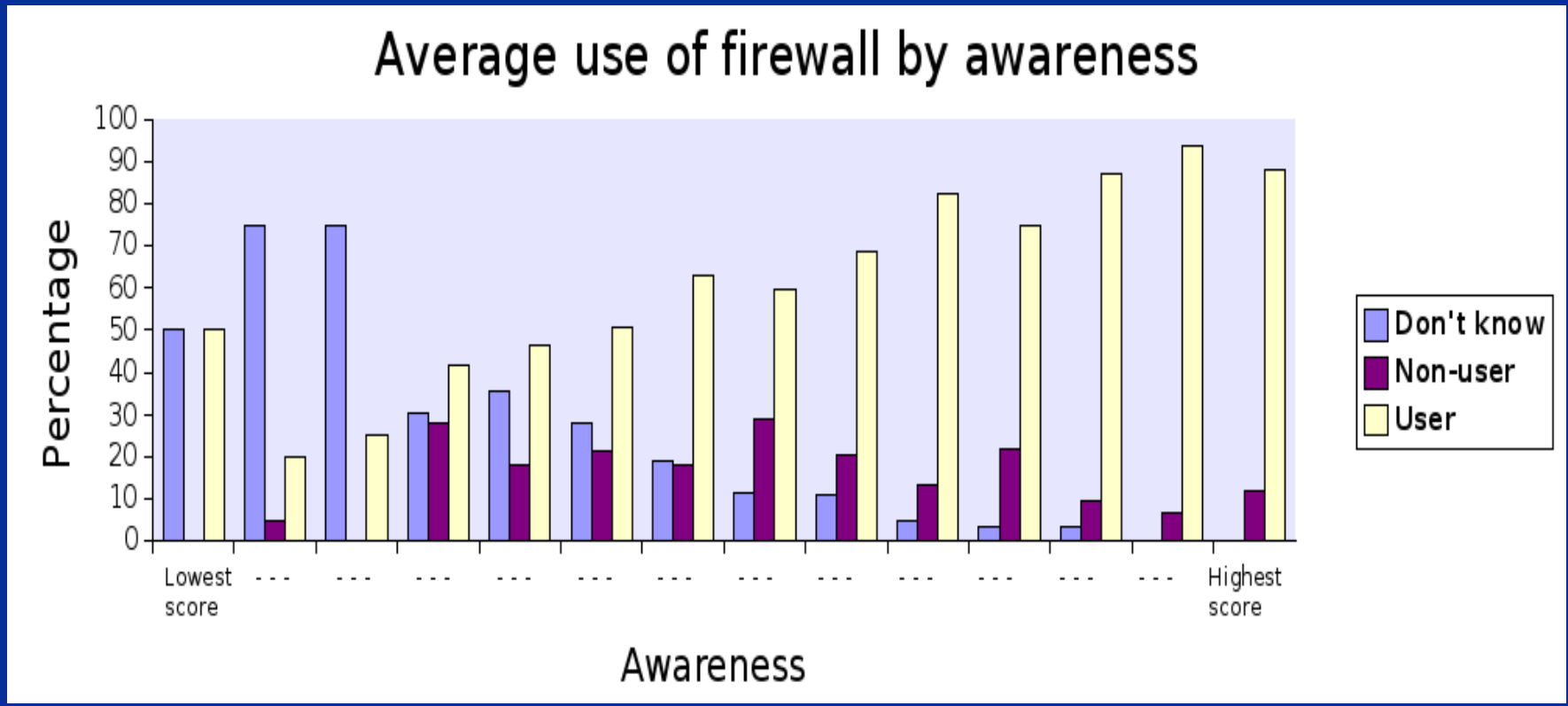
In the second quarter of 2006, close to x% of checked U.S. home computers contained forms of spyware.

Who uses Anti Virus (AV) SW



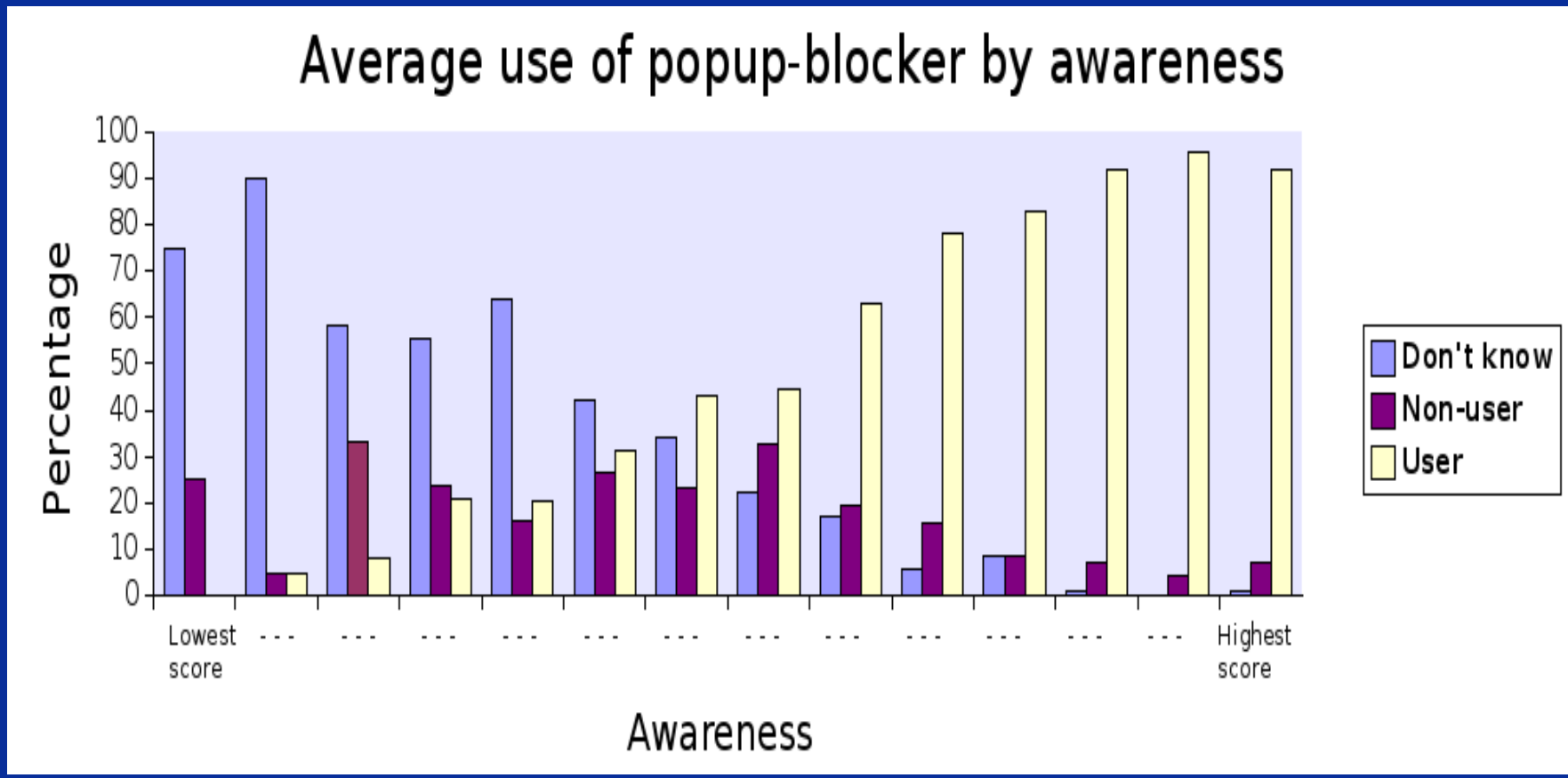
- In total: 92.1% uses AS SW -> OK !

Who uses Firewalls (FW)



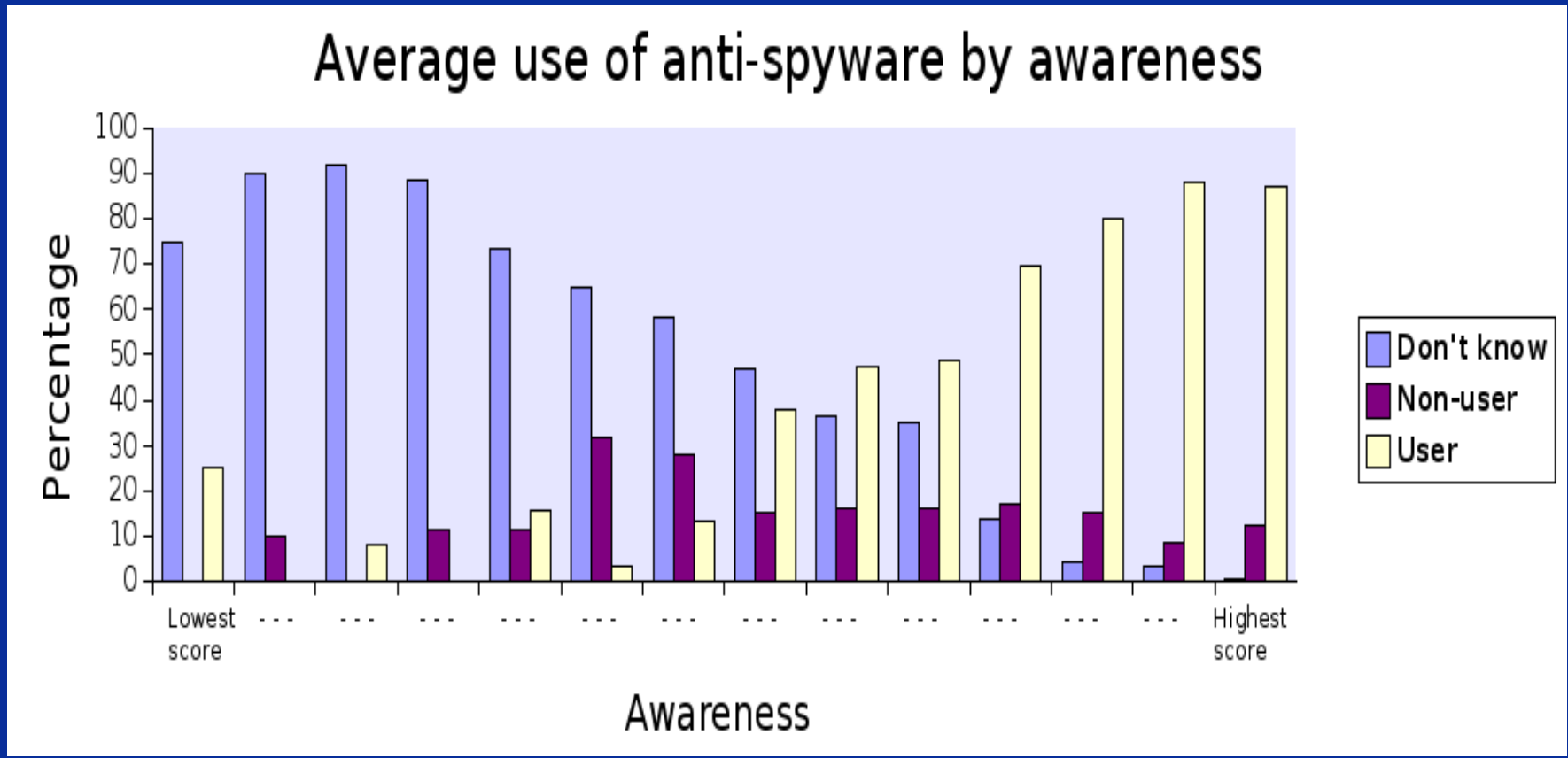
- **In total: 72% uses a FW -> OK !**

Who uses Pop-Up Blockers



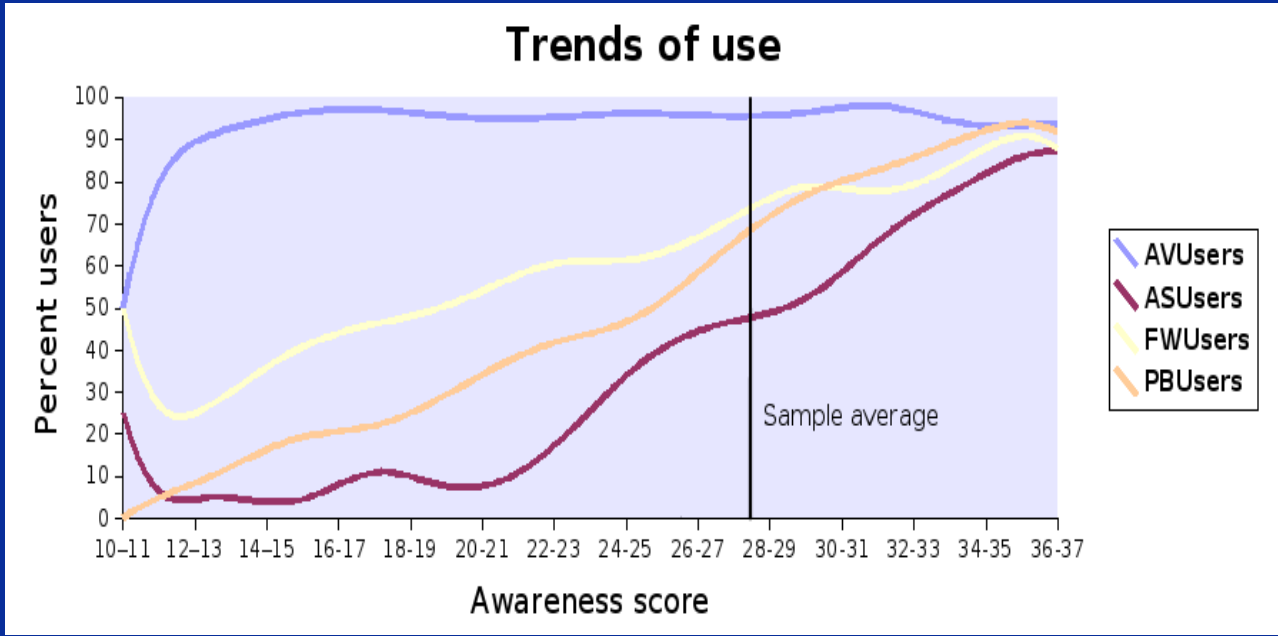
- **In total: 66 % uses AS SW -> fair !**

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 !!

An hypothesis about End Users

Assumptions

- **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 ???

Privacy Principles

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 Principles (cont.)

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"

Privacy Requirements

Map Principles to Requirements

1. Fundamentals

- Data minimization
  - a priori anonymous
  - data are made persistent only when explicitly required
  - data are erased when no longer needed
- Transparency of processing
  - controller keeps track of ALL processing and informs users about it
- Security
  - the systems shall be adequately secured;
    - use Best Practice,
    - consider cost of implementation
    - UPFRONT threat analysis; security measures, continuous Risk Mgmt

2. Lawfulness of processing

- Legality (e.g. consent)
  - Users must understand that they are entering into a contract
- Special categories of personal data
  - processed only when required by law
- Finality and purpose limitation
  - Users have a right to object to processing
- Data quality
  - accuracy, completeness and inspection
  - storage terms
  - periodical clearing

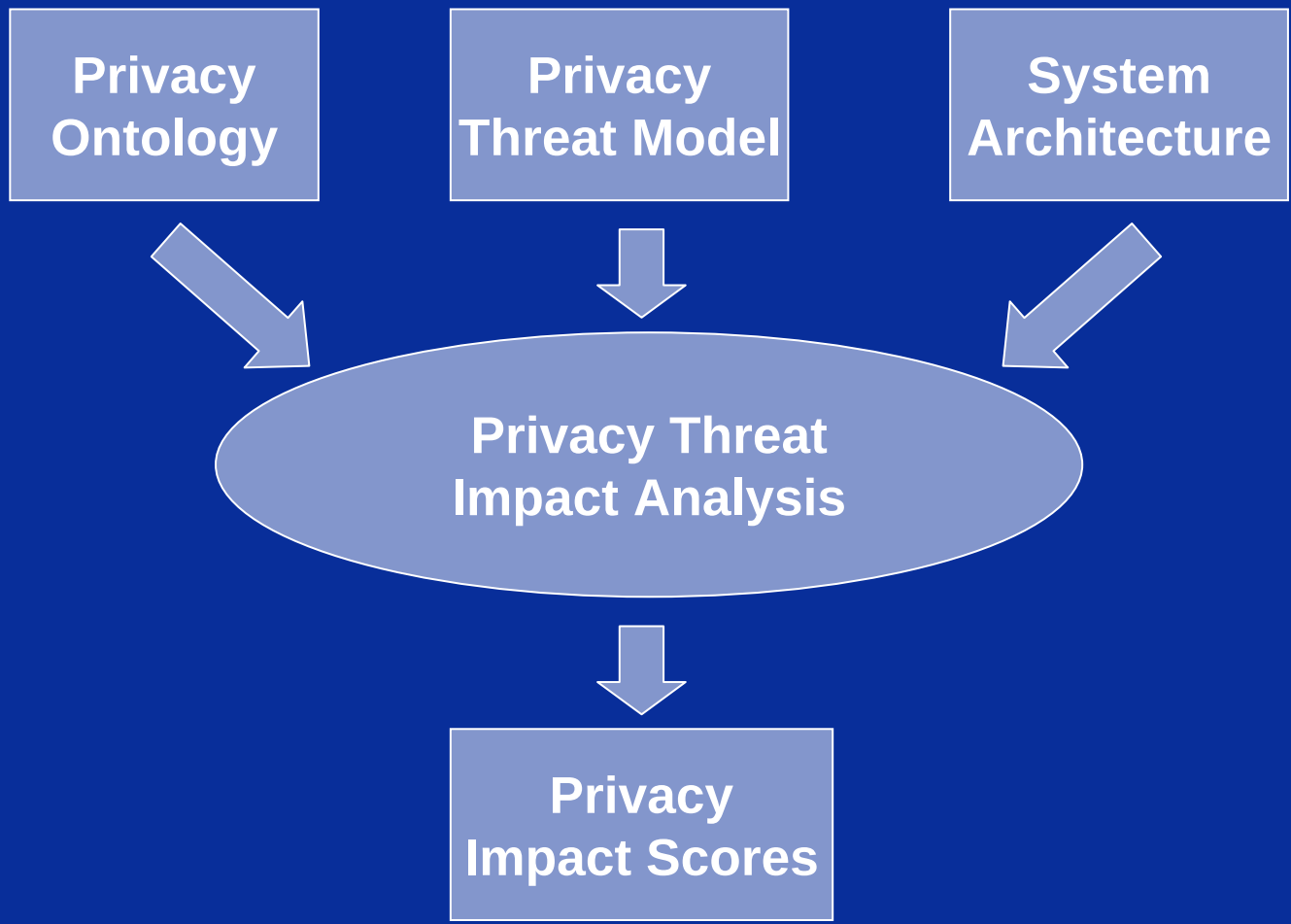
Methods & Tools

- Privacy Ontology
- Privacy Threat model
  - identifies PRIVACY and SECURITY threats
- System Architecture
  - identifies the ASSETS involved
- Threat Impact Analysis
  - evaluate threat IMPACT for each asset

Goal

- Input data to a tool that gives different “views” of the threat model => Privacy Impact Analysis

PETweb Methods & Tools

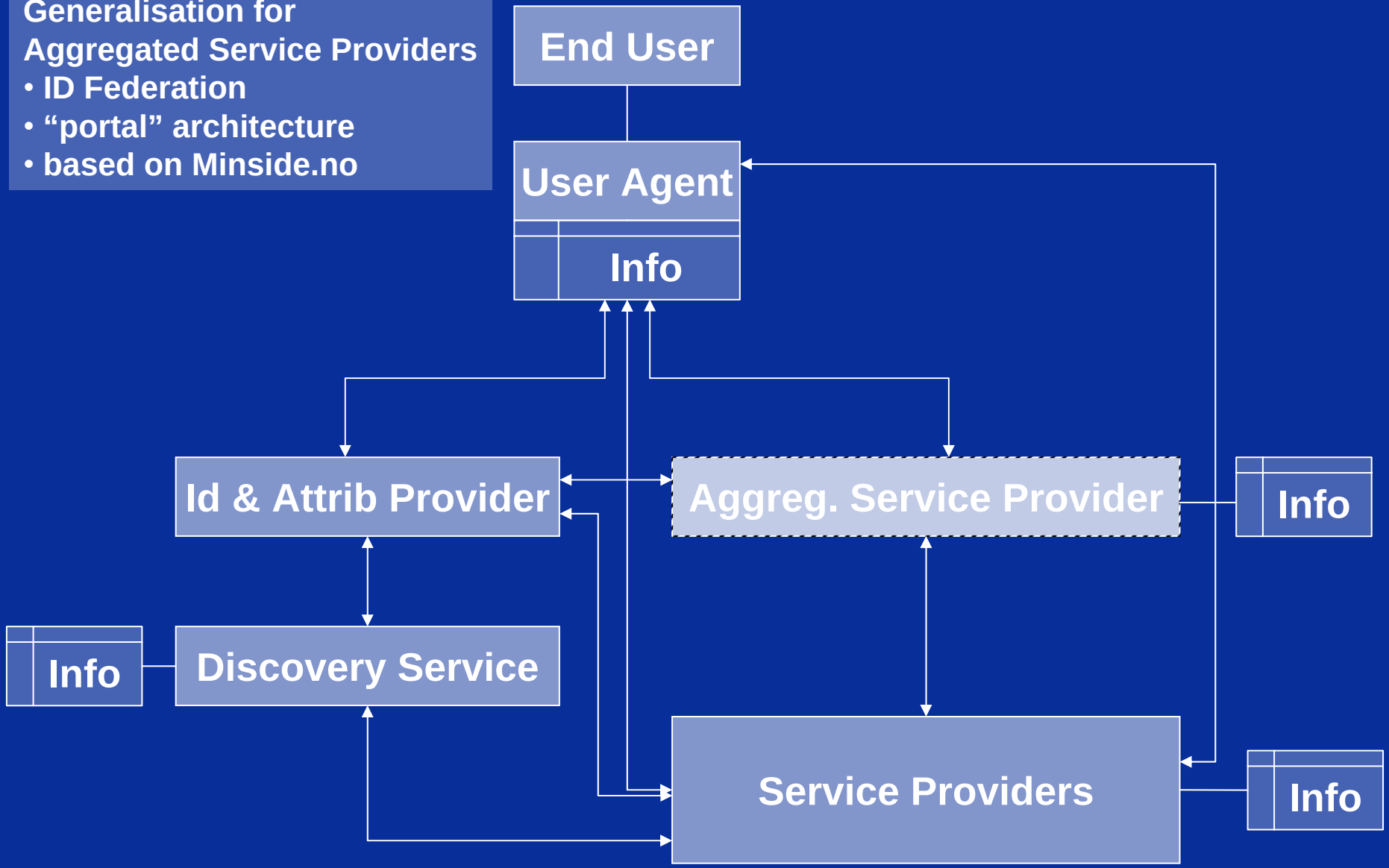


Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

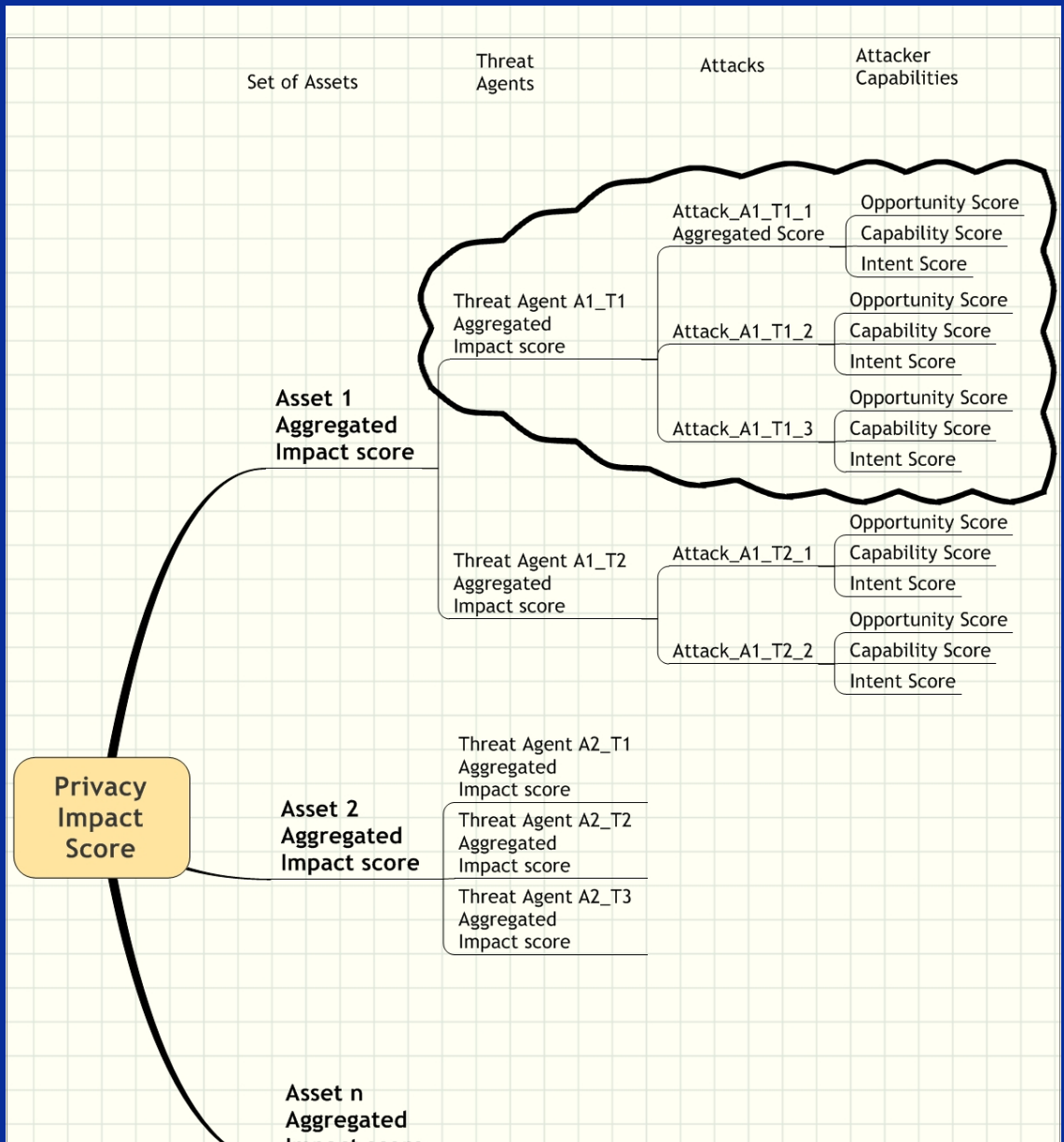
www.nr.no

The PETweb Architecture

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



Privacy Impact Analysis (1)



Privacy Impact Analysis Tool

ber	Asset Name		Rating	Asset Weight	system Rating							
1	**End User (EU)**		100	14,00 %	14							
		max-tas	**avg-tas**	sum-tas								
	Threat Agent type		Impact Score	Threat Weight	Threat weighted Score							
	Hacker threats		5,00	20	100							
	Impact scores:	max	avg	sum(avg)								
		5,00	4,26	12,79								
	Threat Description											
	This measures to what extent a Hacker is a threat to the User Agent and the information on it.											
		Attacks originating from a Hacker										
		Social engineering				Spoofing				Eavesdropping		
	result (floored to 5)	5,00	4,50			5,00	4,96			5,00	3,33	
		max	avg			max	avg			max	avg	
	- Attack Properties											
	Automated/manual A1	0,90	0,90	careful !		1,00	1,00			0,80	0,80	
	Active/passive A2	1,00	1,00	0,1 - 2,0		1,00	1,00	0,1 - 2,0		1,00	1,00	0,1 - 2,0
	(Logical/physical)	1	1			1	1			1	1	
	(Internal/external)	1	1			1	1			1	1	
	- Threat Agent Properties	4	2,16	54		3,2	2,18	54,4		2,8	1,80	45
		max	avg	sum		max	avg	sum		max	avg	sum
	Intent	4	2,8	14		4	3	15		3	2,6	13
	Profit orientation	1				4				3		
	Revenge	4				2				2		
	Vandalism	4				4				3		
	Ego	4				2				2		
	Curiosity	1				3				3		
	Capabilities	4	3,2	16		4	3,4	17		4	3,4	17
	Time ressources	3				3				4		
	Education / Knowledge	4				4				4		
	Financial resources	1				3				2		
	Equipment	4				3				3		
	Skills	4				4				4		
	Opportunity	5	3,6	18		4	3,4	17		4	3	15
	Target Access	5				4				4		
	Target Vulnerabilities	3				3				2		
	Assessed Target weakness	3				4				4		
	Expected attack value / gain	3				2				1		
	Chance of not being caught	4				4				4		
		MAX	AVG			MAX	AVG			MAX	AVG	
	Consequence/Outcome	4,5	2,3125			3,5	2,28125			4,5	2,3125	
		max	avg			max	avg			max	avg	
	- Security Privacy	4	2,25			3	2			4	2,25	
	Interception	1				2				4		
	Manipulation	3				3				2		
	Denial of service	4				1				2		
	Repudiation	1				2				1		
	- Information Privacy	5	2,375			4	2,5625			5	2,375	
	Information collection											
	Surveillance	4		fine		2				2		
	Interrogation	1		fine		1				1		
	Information processing											

Summary

Background

- Awareness study => many users without adequate security

The Framework provides

- Collection of Privacy **Principles** & Structured **Requirements**
- **A knowledge base** that can be maintained with the
  - Privacy Ontology
  - Privacy Threat Model
- **Adaption** to other systems by modifying the
  - System Architecture and Assets involved
  - Privacy Impact Analysis tool
- Different **views of privacy impact** on assets by the
  - Threat Impact Analysis tool

… slutt

Takk for oppmerksomheten !

asmund.skomedal@nr.no

petweb.nr.no