“Identity and Privacy in the Internet Age”

Risks of exchanging identity information

Topics: Privacy, authentication and open issues

Åsmund Skomedal

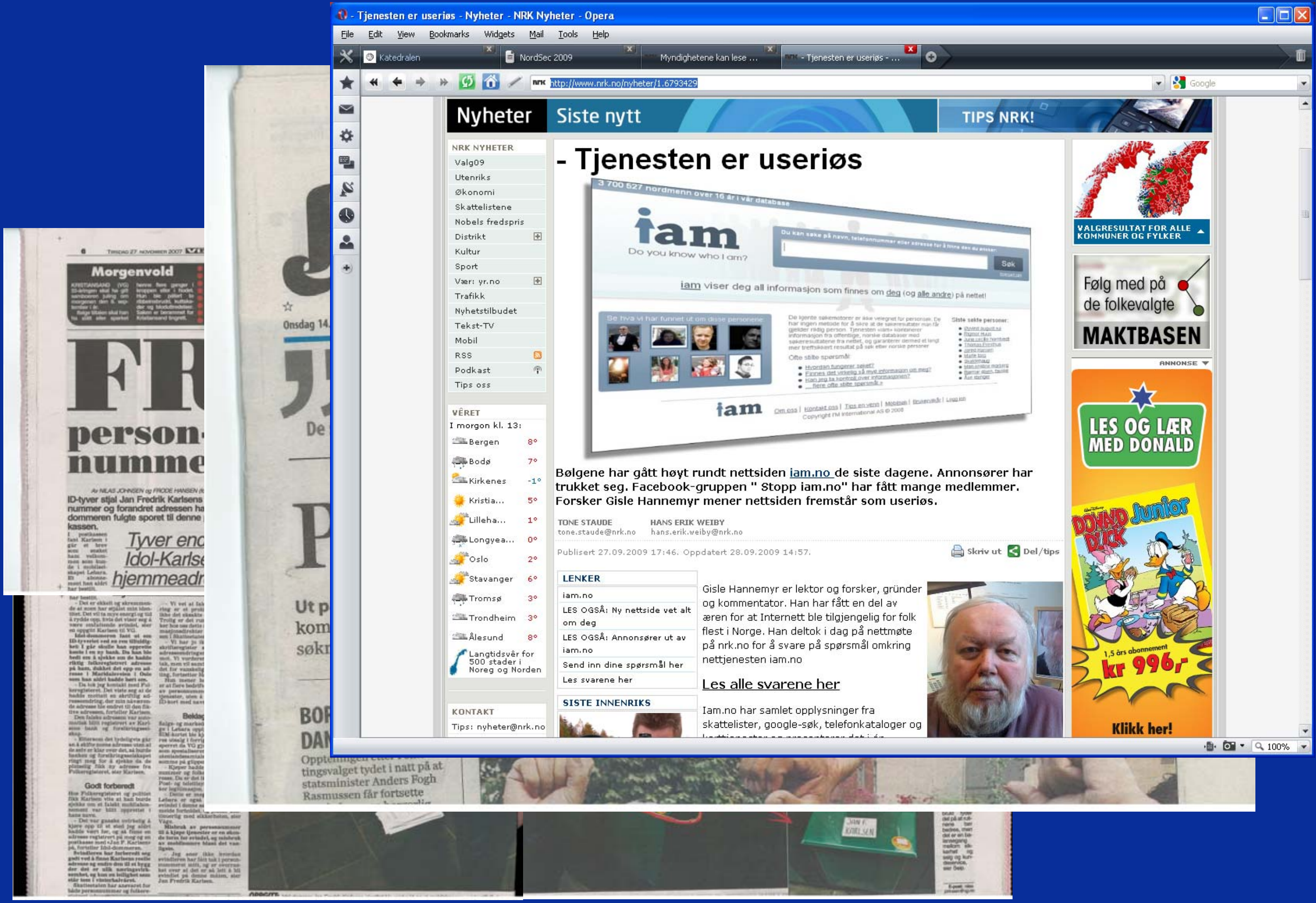
Research Director, Norsk Regnesentral

Nordic Security Day, Oslo, Norway
14. November 2009

Overview

- ► Security vs Privacy risk
- ► PETweb Architecture & threat modelling
- ► Awareness and Protection
- ► Another view on risk
- ► Design faults
- ► Open issues & the future

Privacy & Security in the news …



- Tjenesten er useriøs

Bølgene har gått høyt rundt nettsiden iam.no de siste dagene. Annonsører har trukket seg. Facebook-gruppen " Stopp iam.no" har fått mange medlemmer. Forsker Gisle Hannemyr mener nettsiden fremstår som useriøs.

TONE STAUDE
tone.staude@nrk.no

HANS ERIK WEIBY
hans.erik.weiby@nrk.no

Publisert 27.09.2009 17:46. Oppdatert 28.09.2009 14:57.

LENKER

- iam.no
- LES OGSÅ: Ny nettside vet alt om deg
- LES OGSÅ: Annonsører ut av iam.no
- Send inn dine spørsmål her
- Les svarene her

SISTE INNENRIKS

Gisle Hannemyr er lektor og forsker, gründer og kommentator. Han har fått en del av æren for at Internett ble tilgjengelig for folk flest i Norge. Han deltok i dag på nettmøte på nrk.no for å svare på spørsmål omkring nettjenesten iam.no

Les alle svarene her

Iam.no har samlet opplysninger fra skattelister, google-søk, telefonkataloger og

Security & Privacy issues …

SECURITY properties

- Authentic, Controlled access
- Conf, Integrity, Non Repudiation
- Availability, Audit, Assurance, …

PRIVACY

- Correct info - errors, changes, …
- Purpose - use only for original purpose(s)
- Data minimisation - deleted / revoked after use

Security & Privacy threats …

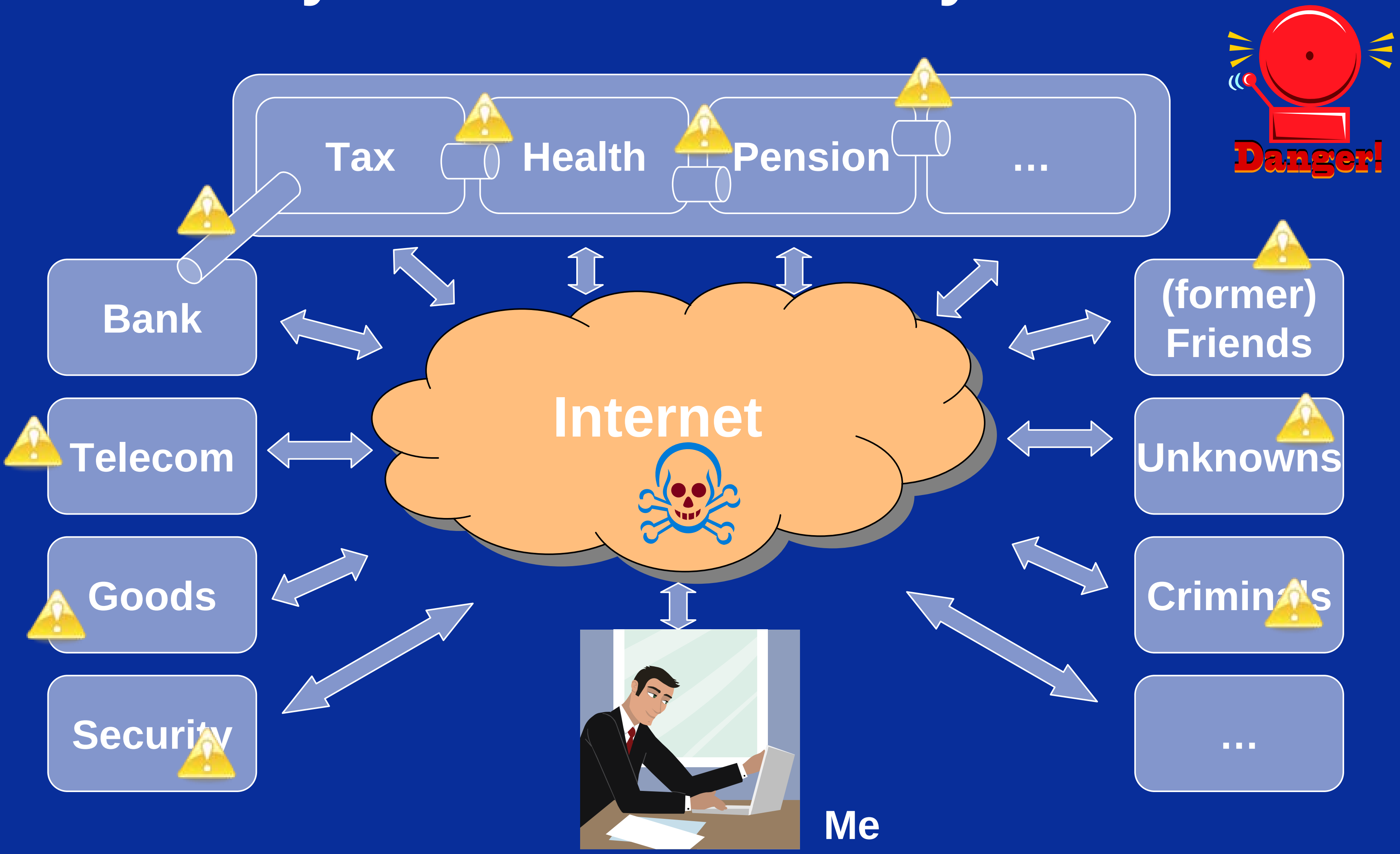
SECURITY

- Masquerade, Unauthorised access
- Interception, Manipulation
- Repudiation, Denial of service, …

PRIVACY

- Processing
  - Incorrect information, notification, transparency
  - Function creep; adding secondary usage
- Collection
  - Storing unused information, nice to have, … misuse (?)
  - Illegal collection (surveillance, …)
- Dissemination
  - Illegal disclosure, exposure,

Identity information is everywhere …



Tax

Health

Pension

…

Danger!

Bank

Telecom

Goods

Security

Internet

(former) Friends

Unknowns

Criminals

…

Me

Some privacy issues from the overall picture

Commercial business applications

- ► Save cost and time; poor data minimization, transparency and controls
- ► “Creative” use of identity information; bend rules as this is an asset
- ► Phishing attacks are enabled by the web itself

Government applications

- ► Tend to exchange or store information without informing end-users … as the “benefit” outweighs the inconvenience for the individual – or does it?
- ► Even more eager to save cost & time …

Consumers / Individuals

- ► All friends are not for a lifetime …
- ► Known and anonymous friends may be unknowingly part of a bot-net
- ► Significant risk that your own protective measures are
  - ▪ too little
  - ▪ too late

because …

Privacy goals are not so operational

BEFORE exchanging IDENTITY information; Terms & conditions, predictability, …

► understand the consequences of using “this service”

► primary usage, agree on this upfront
(treatment, pay for goods/services, anything, …)

DURING exchange; mainly std security stuff - good privacy requires good security

► good access controls for “super users” (!)

► storing only relevant and required information

AFTER exchange; only use for original purpose, update info and controlled use

► have clear limits on “customer record” information flow

► no dissemination of information with other “agencies” or “partners”

► a clear view on what the purpose is and monitor “this service” evolve
(and do NOT add a new purpose - with or without intention)

► update the information so that it reflects reality

► do NOT keep it forever … just to be on the safe side

How to understand privacy risk

Starts with a

“system”

that has

vulnerabilities

and is exposed to

threats

causing an estimated

impact

giving rise to a

risk !

for privacy violation

Privacy RISKS - how to understand them

Need a

- ► “system” (i.e. an architecture)

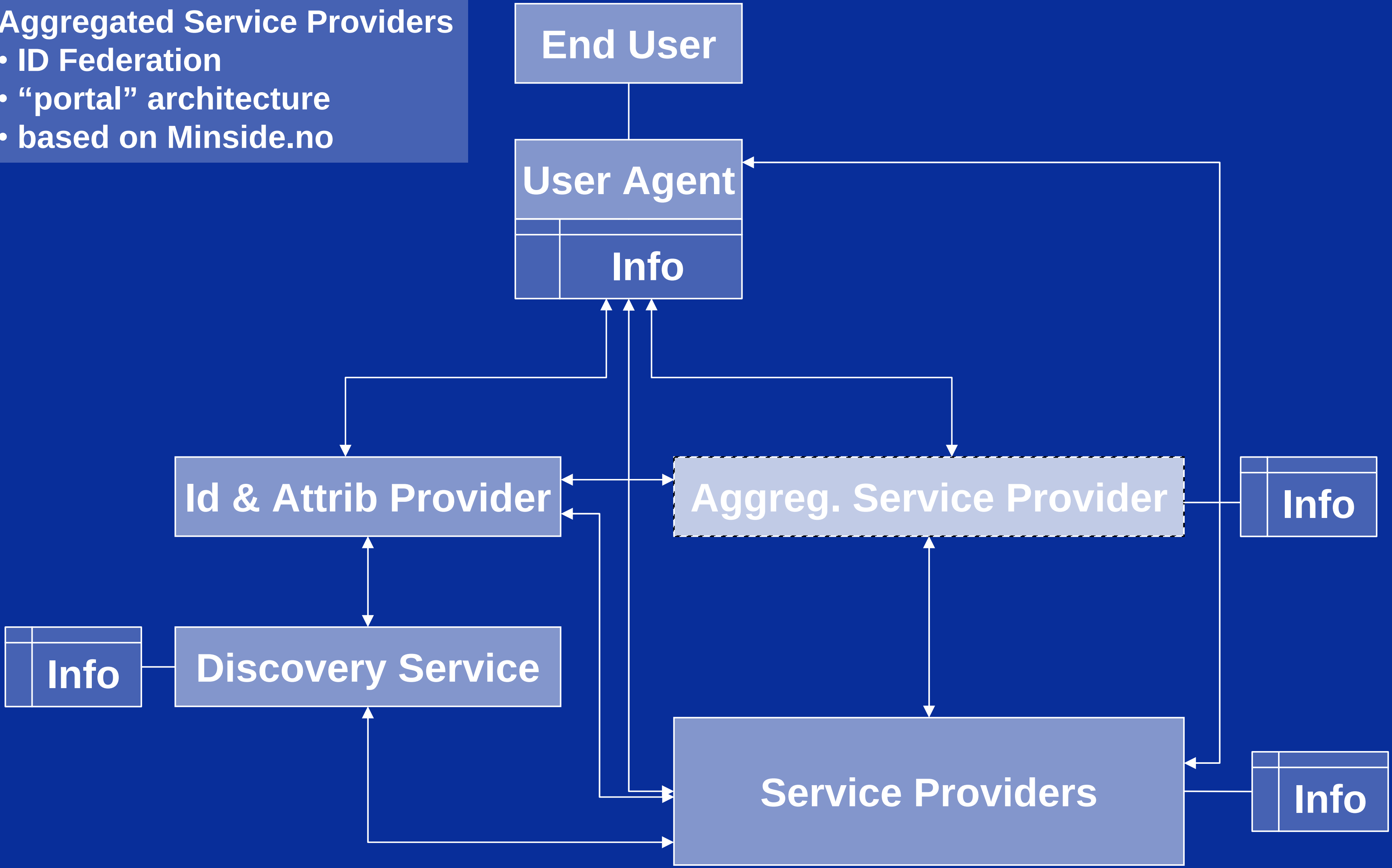
that has

- ► vulnerabilities; where are the WEAK PARTS ???

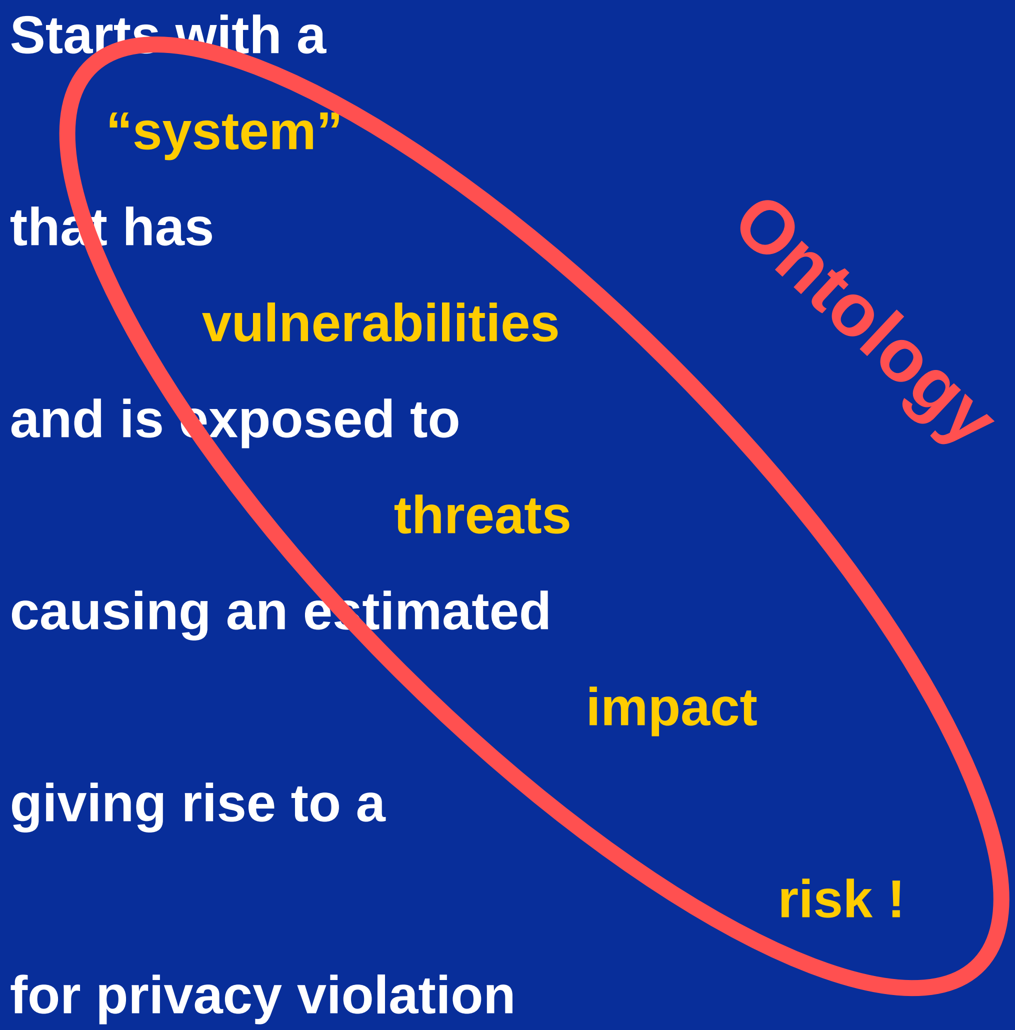
… here is an architecture (from the PETweb project)

The PETweb Architecture

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



How to understand privacy risk



Starts with a

“system”

that has

vulnerabilities

and is exposed to

threats

causing an estimated

impact

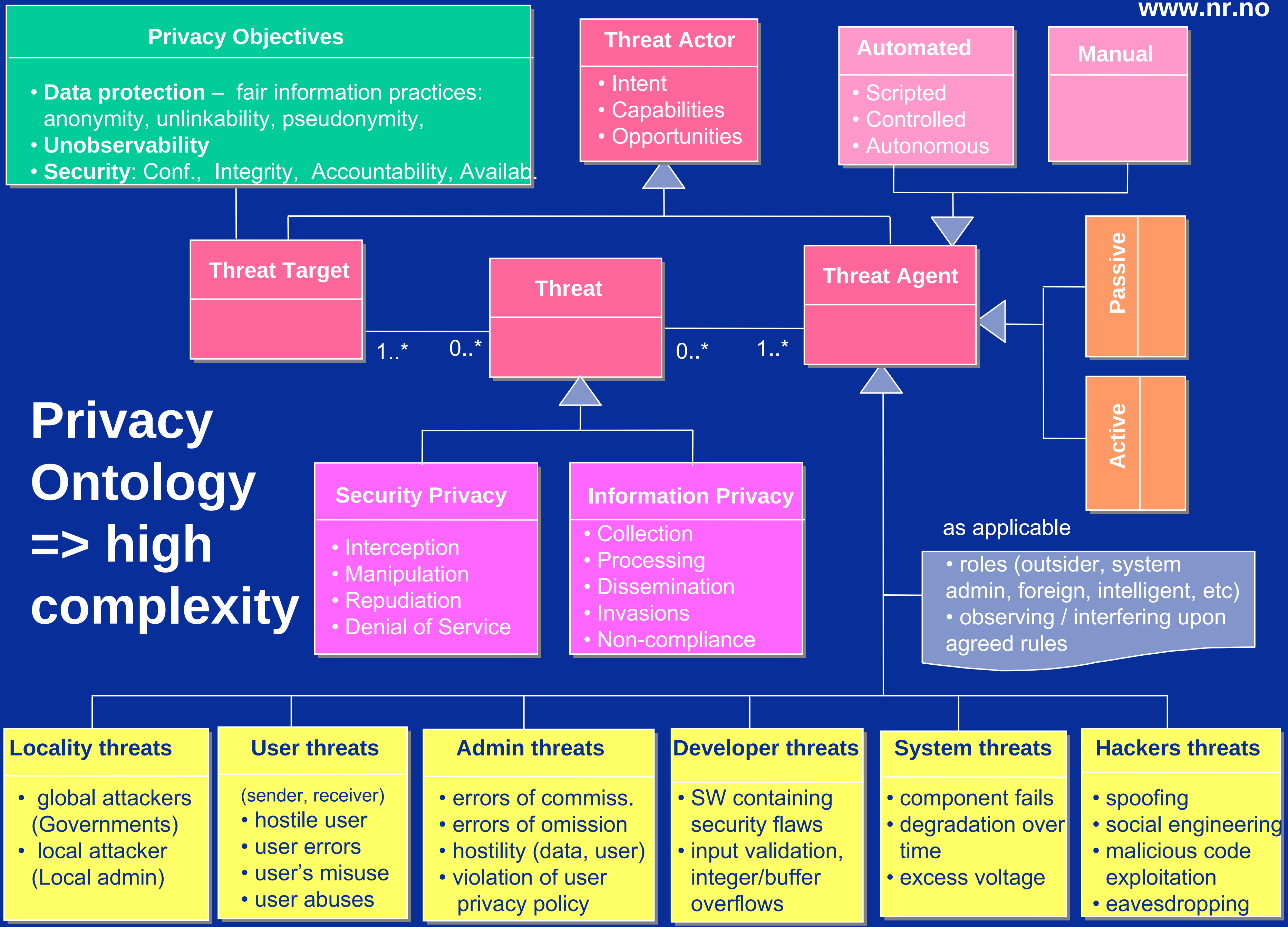
giving rise to a

risk !

for privacy violation

www.nr.no

Privacy Ontology => high complexity



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

Threat Target

1..*

0..*

Threat

0..*

1..*

Threat Agent

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

How to understand privacy risk

Starts with a

“system”

that has

vulnerabilities

and is exposed to

threats

causing an estimated

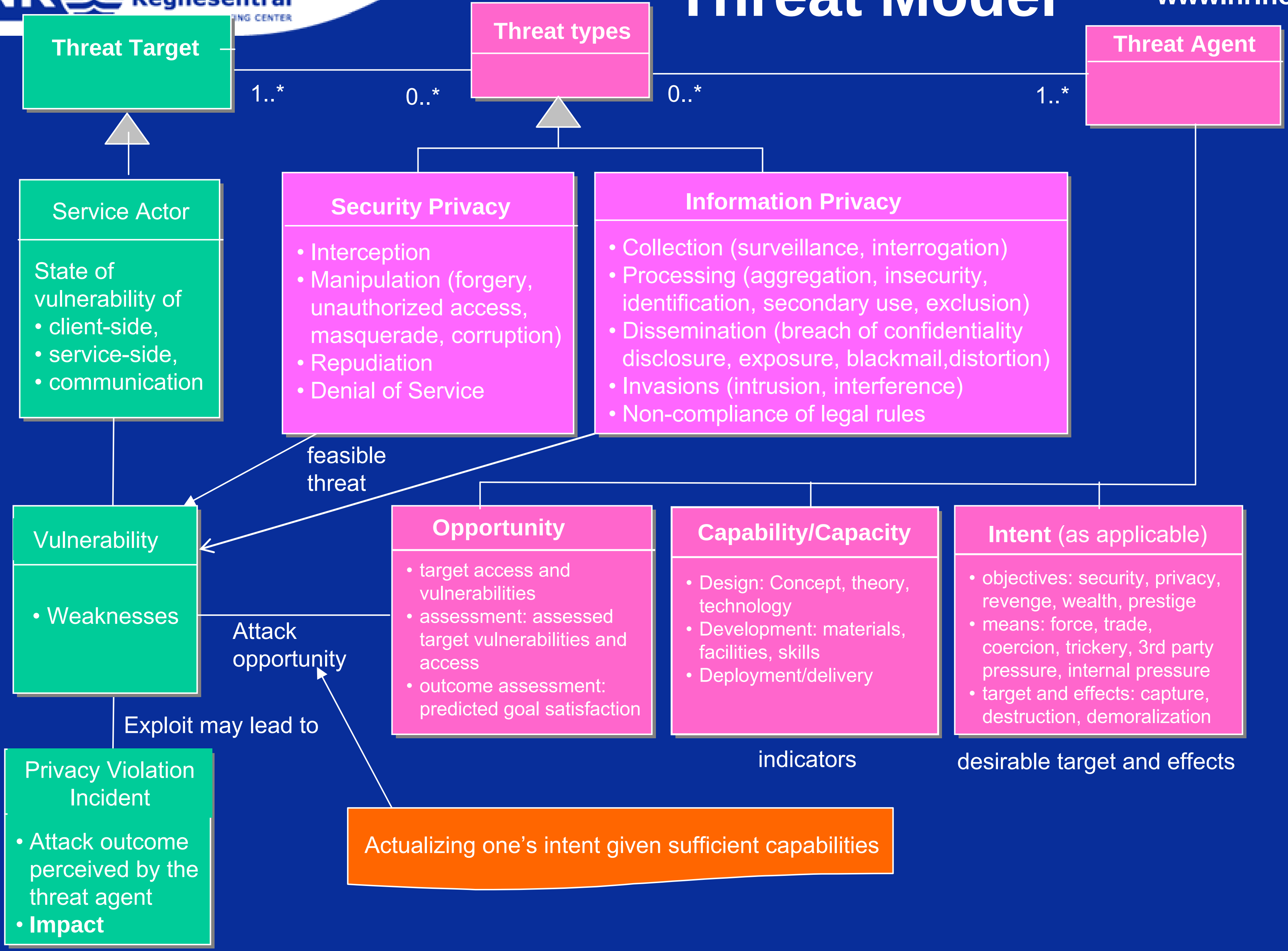
impact

giving rise to a

risk !

for privacy violation

Threat Model



Threat Target

1..*

0..*

Threat types

0..*

1..*

Threat Agent

Service Actor

State of vulnerability of
- client-side,
- service-side,
- communication

Security Privacy
- Interception
- Manipulation (forgery, unauthorized access, masquerade, corruption)
- Repudiation
- Denial of Service

Information Privacy
- Collection (surveillance, interrogation)
- Processing (aggregation, insecurity, identification, secondary use, exclusion)
- Dissemination (breach of confidentiality disclosure, exposure, blackmail,distortion)
- Invasions (intrusion, interference)
- Non-compliance of legal rules

feasible threat

Vulnerability
- Weaknesses

Attack opportunity

Opportunity
- target access and vulnerabilities
- assessment: assessed target vulnerabilities and access
- outcome assessment: predicted goal satisfaction

Capability/Capacity
- Design: Concept, theory, technology
- Development: materials, facilities, skills
- Deployment/delivery

Intent (as applicable)
- objectives: security, privacy, revenge, wealth, prestige
- means: force, trade, coercion, trickery, 3rd party pressure, internal pressure
- target and effects: capture, destruction, demoralization

indicators

desirable target and effects

Exploit may lead to

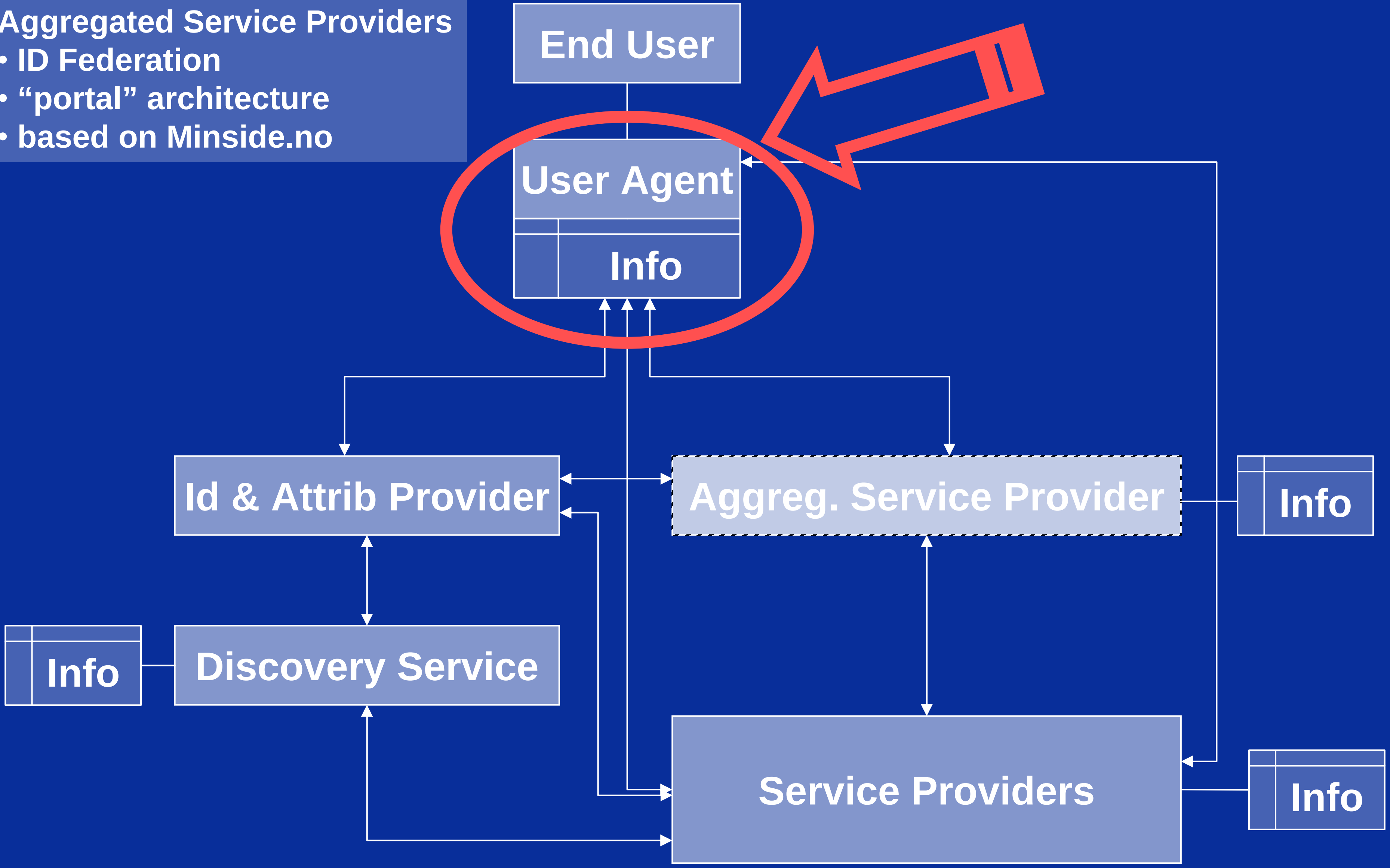
Privacy Violation Incident
- Attack outcome perceived by the threat agent
- **Impact**

Actualizing one’s intent given sufficient capabilities

The PETweb Architecture

Generalisation for Aggregated Service Providers

- ID Federation
- “portal” architecture
- based on Minside.no



Privacy – User Agent vulnerabilities

There is a large responsibility for each citizen to have an updated security regime on the User Agent (PC)

The PETweb project revealed that User Agents managed by end-users are vulnerable because …

the actual use of protective measures correlates strongly with end-user awareness

and awareness is not instant (!)

Awareness and Protection

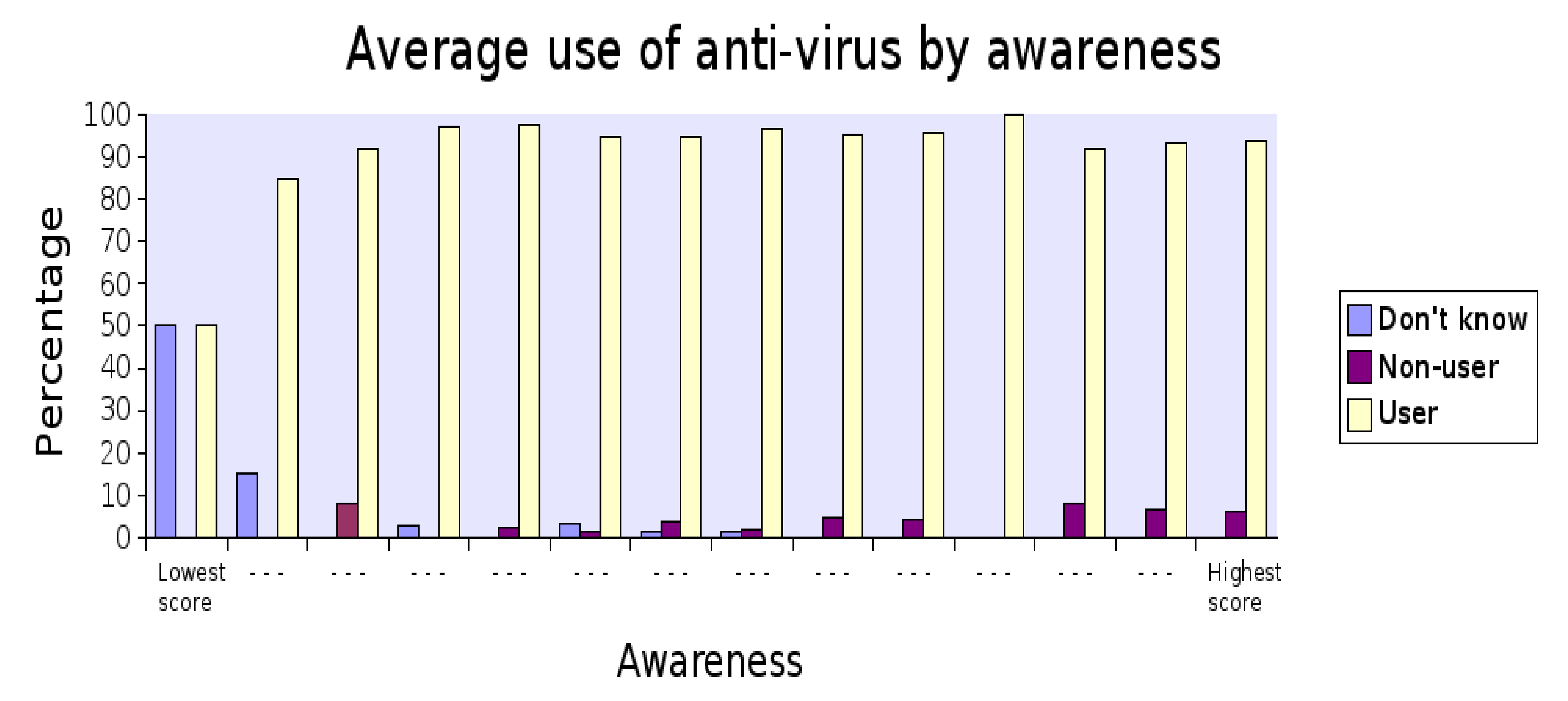
Findings from MSc Thesis of Freddy Andreassen (Høgskolen i Gjøvik, 2007)

- ► Almost everyone knows about viruses and the need to protect against it
- ► 70 % use firewalls and pop-up blockers
- ► 50% use anti spyware SW on average

Why is this a problem?

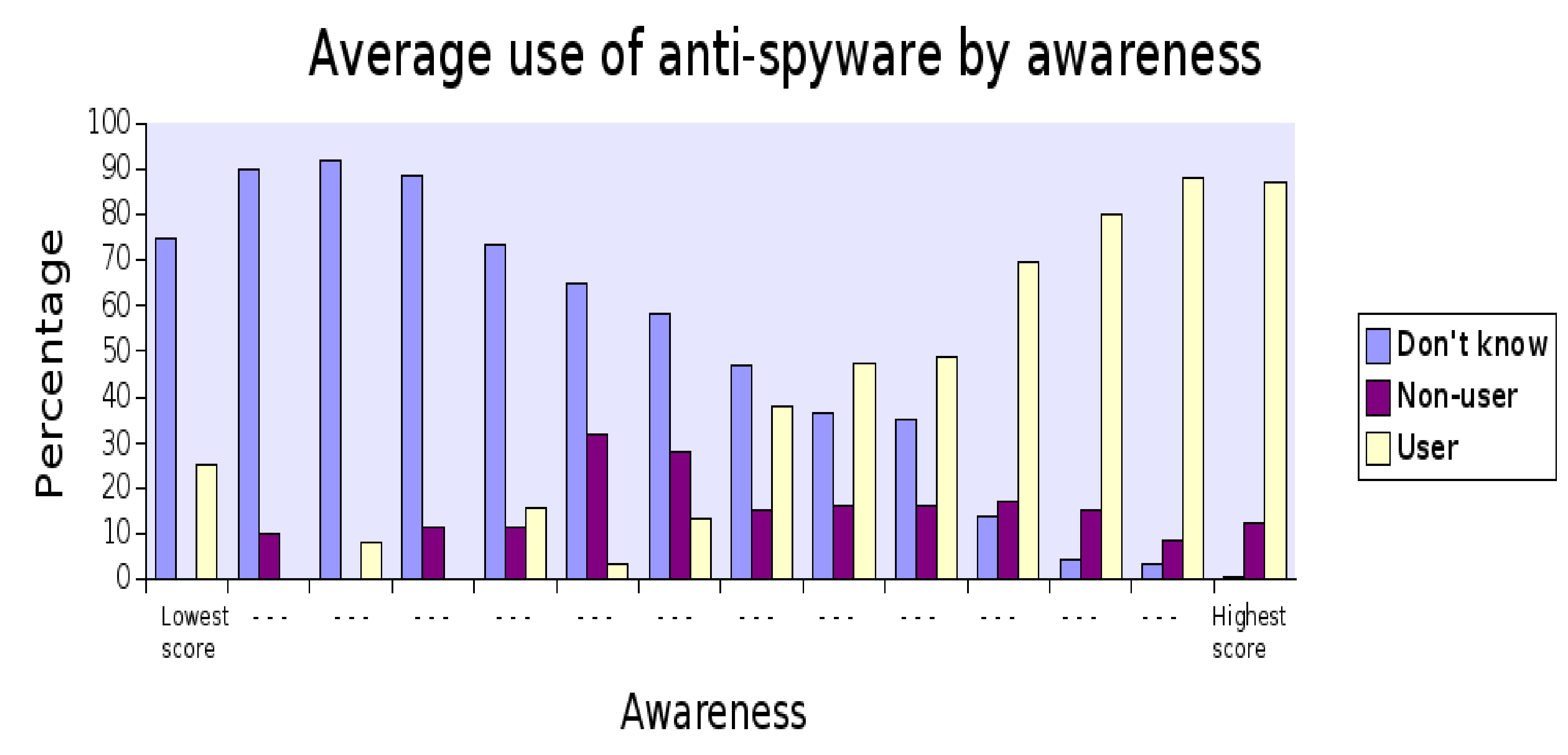
In the second quarter of 2006, close to x% of checked U.S. home computers contained forms of spyware.

Anti Virus



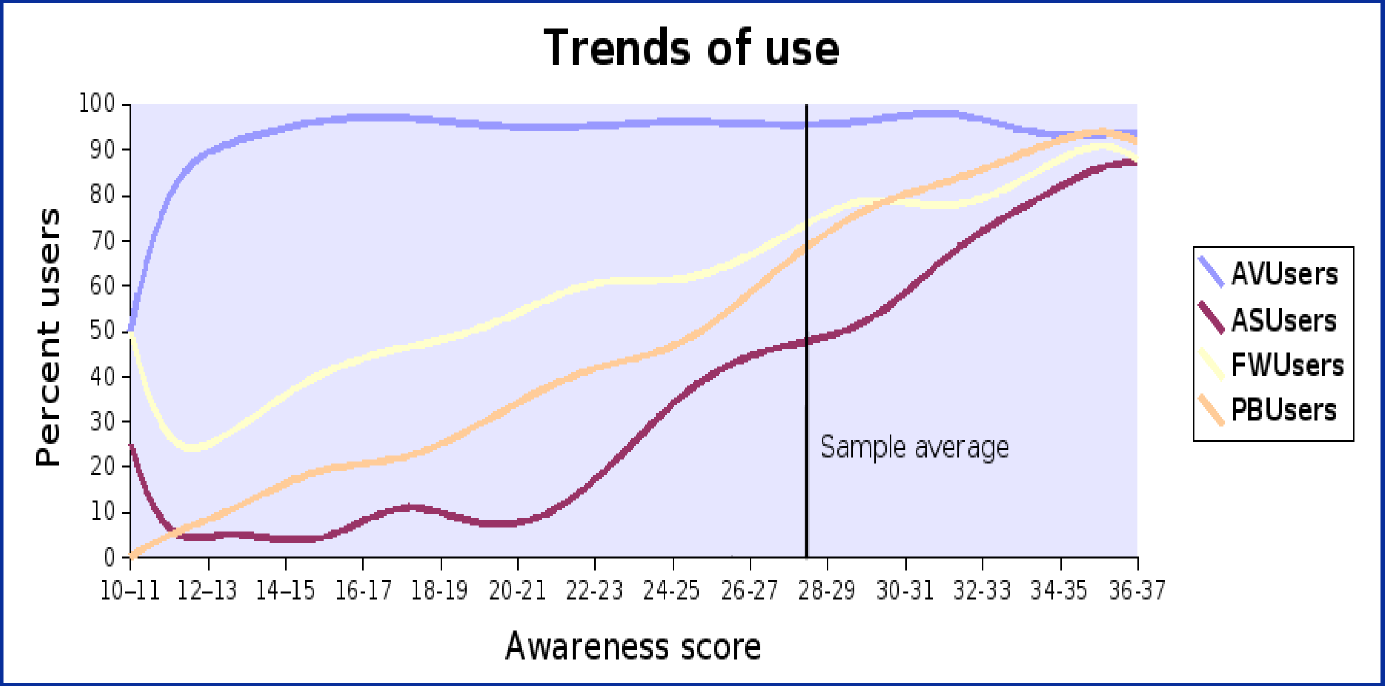
- In total: 92.1% uses AV SW -> OK !

Anti Spyware



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

Awareness and Protection (cont)



In 2006 ~ **90%** of U.S. home computers contained forms of spyware

Best guess
⇒ many get spyware without knowing about the threat
⇒ many get spyware with Anti Spyware installed

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

Privacy RISKS - how to understand them

An architecture were User Agents store identifiers;

poor management is a vulnerability exposed to

attacks (threats) every day.

The possible impact includes identity theft and disclosure

This again implies complex security & privacy breaches;

repeated masquerade

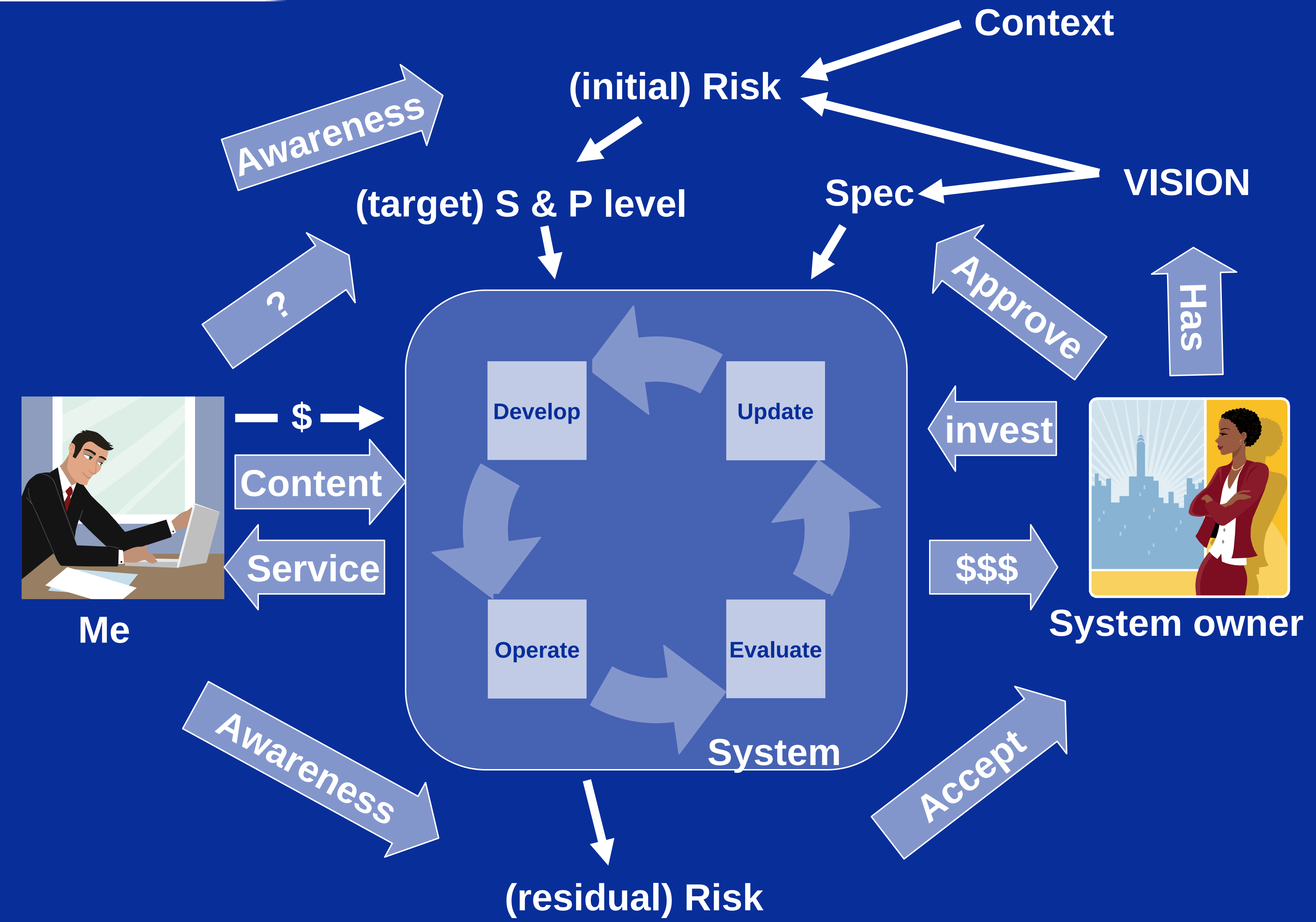
financial loss

breach of privacy of stored SENSITIVE private info

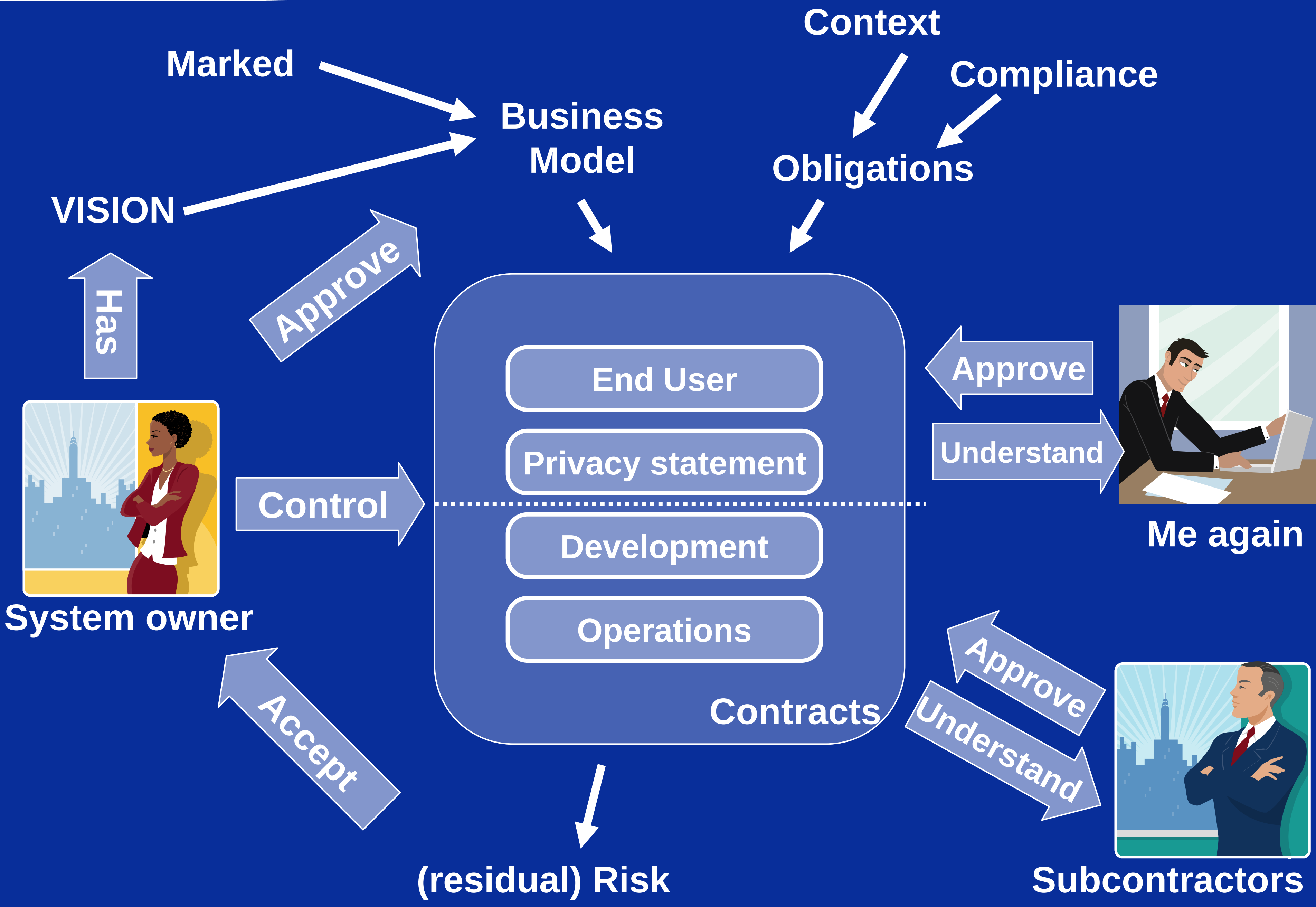
blackmail ?

… and whatever we can think of

Another view on risk



Another view on risk - 2



Marked

VISION

Business Model

Context

Compliance

Obligations

Has

Approve

System owner

Control

End User

Privacy statement

Development

Operations

Contracts

Approve

Understand

Me again

Approve

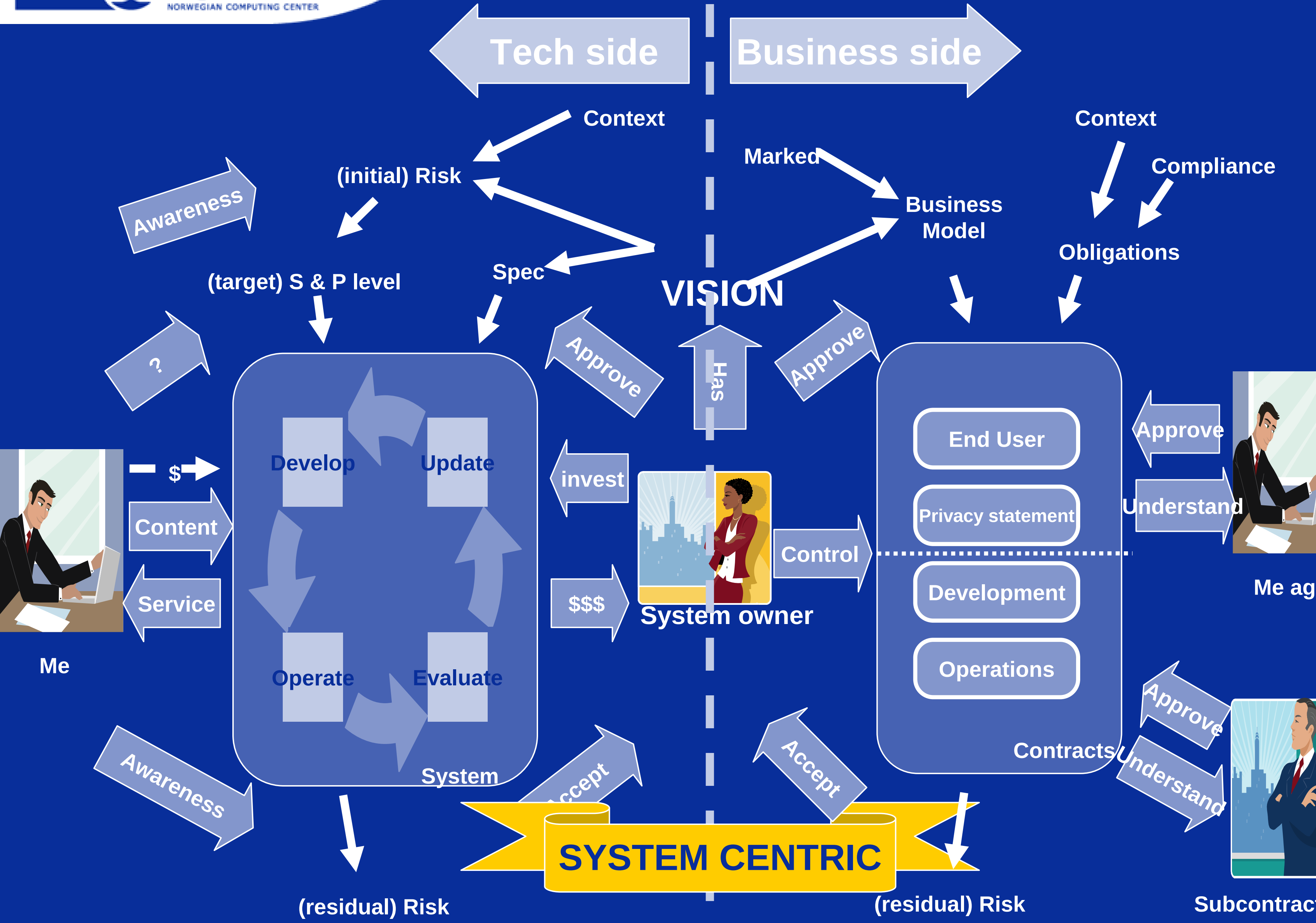
Understand

Subcontractors

Accept

(residual) Risk

Where is the focus?



Tech side

Business side

Context

(initial) Risk

Awareness

(target) S & P level

Spec

Marked

Business Model

Context

Compliance

Obligations

VISION

?

Approve

Has

Approve

Develop

Update

Operate

Evaluate

System

$

Content

Service

Me

invest

$$$

System owner

Control

End User

Privacy statement

Development

Operations

Contracts

Approve

Understand

Me ag

Approve

Understand

Subcontrac

Awareness

Accept

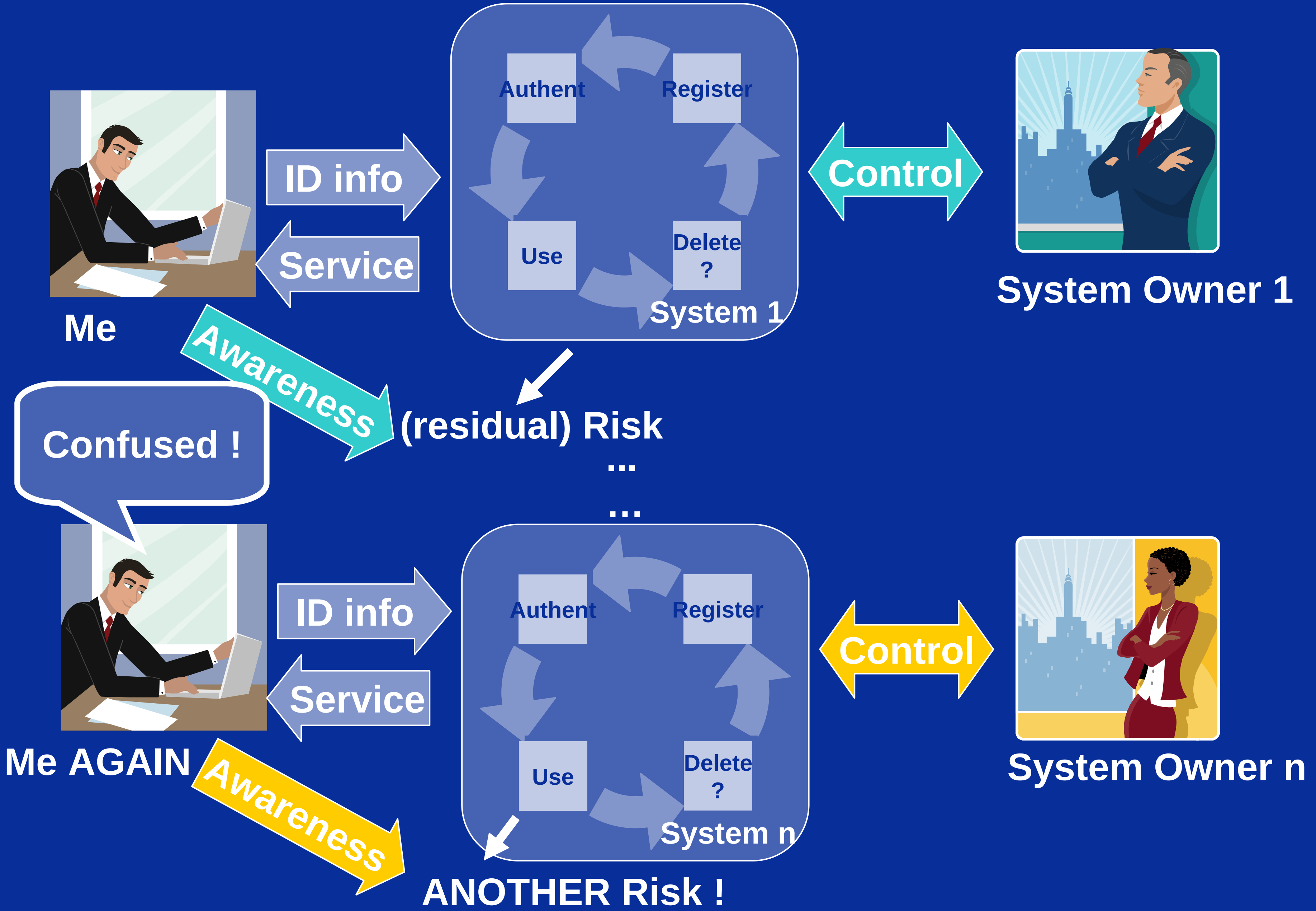
Accept

SYSTEM CENTRIC

(residual) Risk

(residual) Risk

A users view



Me

ID info

Service

Authent

Register

Use

Delete ?

System 1

Control

System Owner 1

Awareness

(residual) Risk

...

...

Confused !

Me AGAIN

ID info

Service

Authent

Register

Use

Delete ?

System n

Control

System Owner n

Awareness

ANOTHER Risk !

Security and Privacy design faults

There are many types of faults in security systems, e.g.

- Use of Identifiers that are guessable
- Security design and implementation is inconsistent
- Design errors
  - high complexity, inconsistent doc
  - incomplete specification and modelling
- Exclusion of significant user groups
  - blind user can not read one-time-passwords
  - dyslectic people can not select “safe” passwords

… and probably many more, so this requires further research

Security and Privacy design faults …

Technical instability

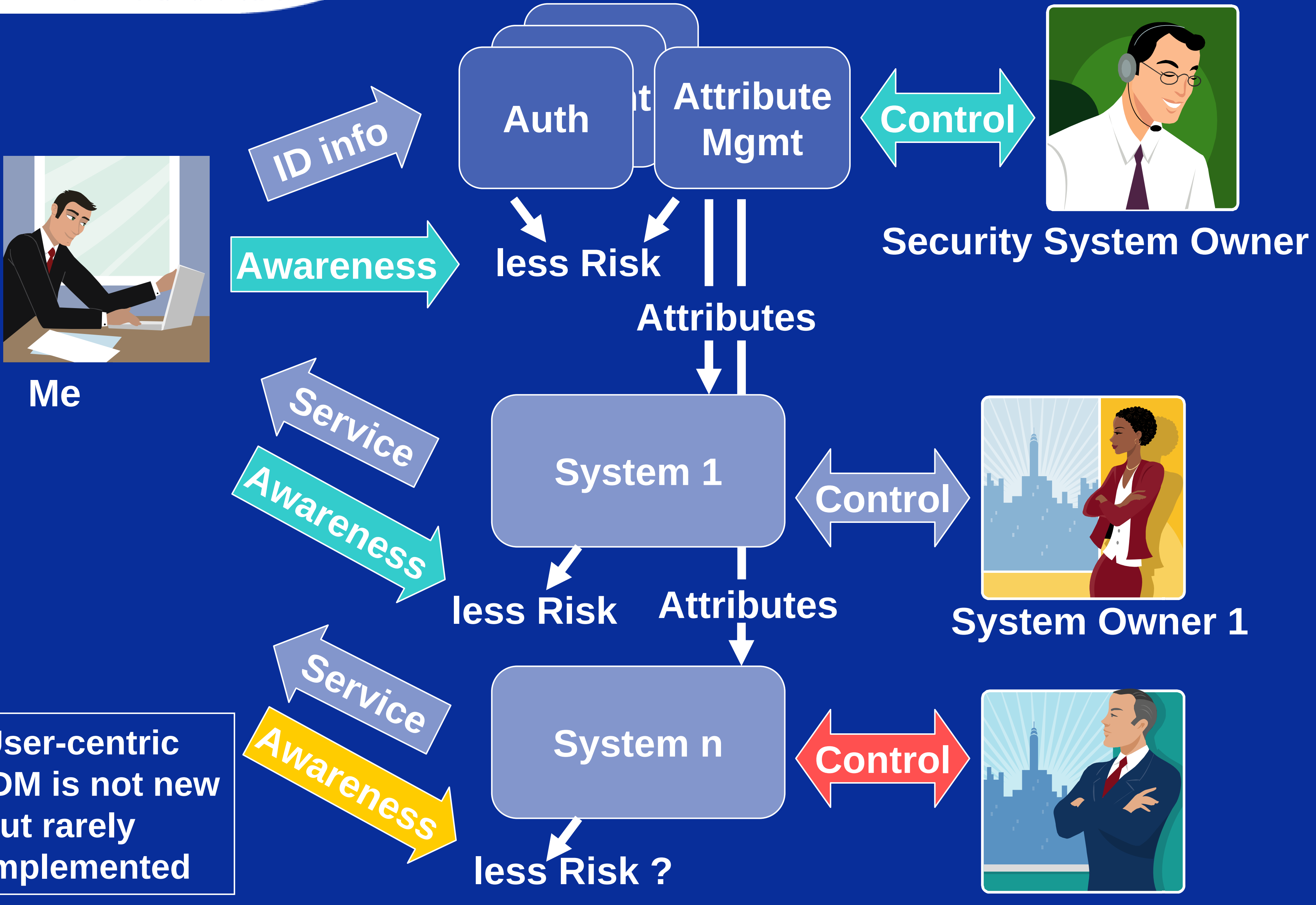
- ▪ changes on authentication procedures and technology
- ▪ migration of systems bit by bit
- ▪ development and testing with REAL data

- ► Immature development environments
- ► Poor HCI capabilities
    - ▪ can not easily convey "risk level" or "security level"
- ► Lack of (international) standards ? (!)
- ► All services have a different Policy

  => considerable confusion

So many security solutions may not be such a good idea?
Is it an alternative is to centralise …

Another approach ...



User-centric IDM is not new but rarely implemented

Attributes can be less sensitive or anonymous!

Some open issues …

The risk of exchanging id information is unpredictable

- ► Technical instability
- ► Immature development environments, lack of PETs
- ► Unsound development methods
- ► Lack of (international) standards ?
  - ▪ Norway: SEID & PKI for Gov Applications (ca 2004 !)
- ► Confusion with different Policy / Business Model
  - ▪ How to create real user-centric IDM solutions
  - ▪ Harmonisation in public sector possible
  - ▪ Will incidents trigger better user Awareness? (recently; iam.no?)

The future of Security and Privacy design?

There is a need to figure out the "dynamics" of security and Privacy; we need to understand better what motivates the end-Users and System owners …

Issue	Now	Future ?
Premises / Control of ID Info	Business	User
Business Model	$$$	Balanced
Obligations (sometime also cost)	Mainly user	Balanced
Control over Service Info	Poor (?)	Owner
Deletion of ID Info (after use)	Poor	Controlled
Function Creep (secondary purpose)	Uncertain	Controlled
Awareness	Low	Better
Risk / security levels	Uncertain	"Classified"

There is hope!

… the end

Thank you for your attention !

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, Karlstad Univ. DIFI, Uninett

References

Here are some references to useful sites and some related documentation …

- petweb.nr.no
- minside.no
- NRK oppslag om “iam.no” tjenesten: http://www.nrk.no/nyheter/1.6793429
- Are the Norwegian Internet users ready for the new threats to their information?
  Freddy Andreassen, MSc Thesis. Gjøvik Univerity College. 2007. http://brage.bibsys.no/hig/handle/URN:NBN:no-bibsys_brage_4220