NST | Norwegian Centre for Telemedicine
UNIVERSITY HOSPITAL OF NORTH NORWAY
WHO Collaborating Centre for Telemedicine

TROMSØ TELEMEDICINE LABORATORY

sfi Centre for Research-based Innovation
Established by the Research Council of Norway

Threats to Information Security of Real-time Disease Surveillance Systems

Presentation for MIE 2009

Eva Henriksen
eva.henriksen@telemed.no

Co-authors: Monika A. Johansen, Anders Baardsgaard, Johan Gustav Bellika

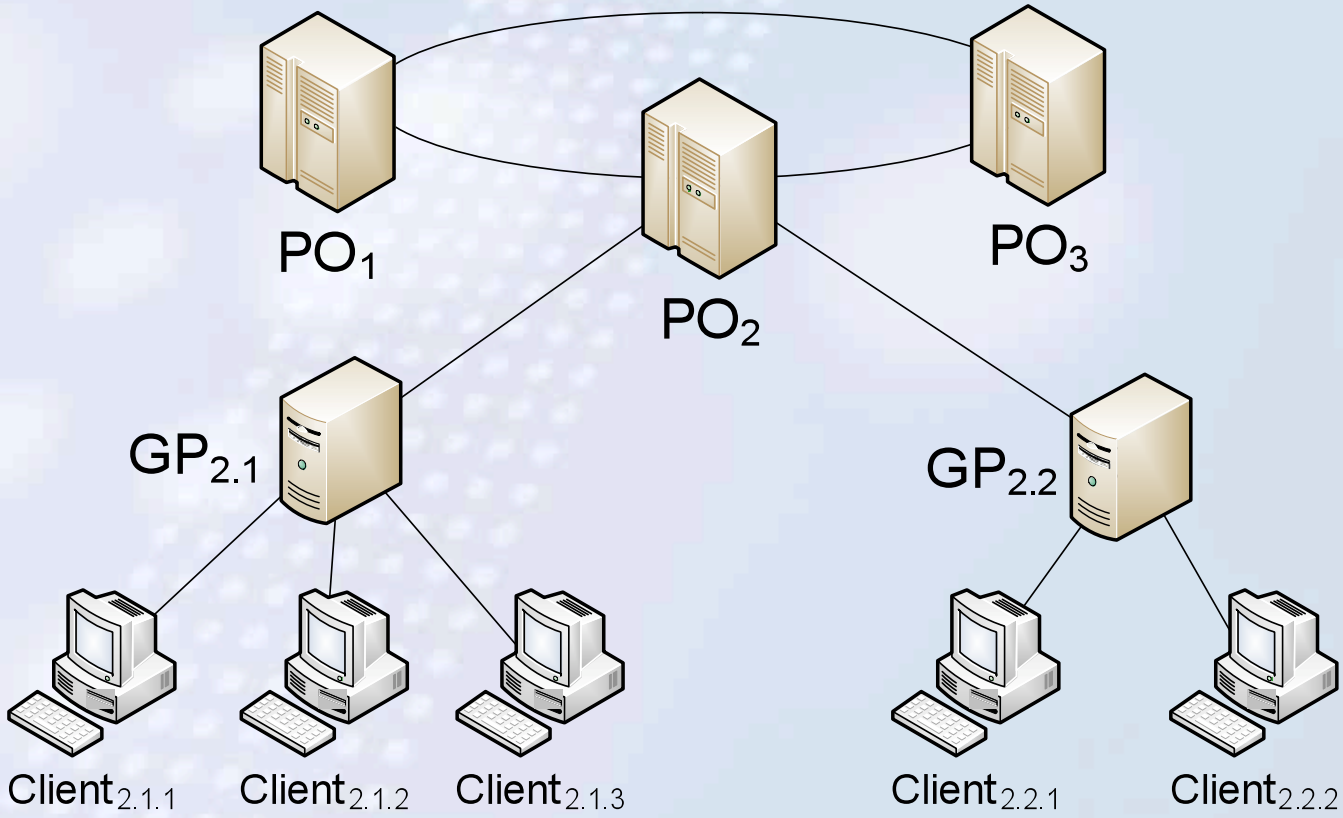
Outline

- The Snow system
- Risk Assessment methodology
- Risk Assessment of the Snow system
  - Requirements and legal baseline
  - Definitions, values
  - Identified threats
  - Likelihood, consequence and risk level

The Snow Agent System

- A real-time peer-to-peer disease surveillance solution
- Extract anonymous data from health service providers in a defined geographic area (e.g. GPs' EHR systems, lab systems)
- Detected outbreaks communicated using instant messaging

An overall model for the Snow system



Legal baseline, security requirements

- Person information, personal data
  - identifies a specific/natural person
- Anonymous information
  - is *not* person identifiable information
- Health information
  - is *sensitive* person information
- Snow:
  - Sensitive personal health information kept at GP offices
  - Only anonymous information is transferred

Risk Assessment (RA) methodology

Main steps:

1. Context identification
   - Target of evaluation; system description; requirements; legal baseline
2. Threat identification
   - Possible unwanted incidents
3. Risk analysis
   - Likelihood, consequence and risk for each threat
4. Risk evaluation
   - Risk level and risk acceptance
5. Risk treatment
   - Proposals for handling the risks

Qualitative values for Likelihood

Likelihood	Frequency	Ease of misuse; motivation
Very high	Very often. Occurs more often than every 10th connection, i.e. more frequently than 10% of the time/cases.	Can be done without any knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
High	Quite often. Occurs between 1% and 10% of the time/ cases.	Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
Moderate	May happen. Occurs between 0.1% and 1% of the time/cases.	Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.
Low	Rare. Occurs less than 0.1% of the time/cases.	Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel.

Qualitative values for Consequence

Consequence	For the patient/citizen	For the service provider
Small	No impact on health; or negligible economic loss which can be restored; or small reduction of reputation in the short run.	No violation of law; or negligible economic loss which can be restored; or small reduction of reputation in the short run.
Moderate	No direct impact on health or a minor temporary impact; or economic loss which can be restored; or small reduction of reputation caused by revealing of less serious health information.	Offence, less serious violation of law which results in a warning or a command; or economic loss which can be restored; or reduction of reputation that may influence trust and respect.
Severe	Reduced health; or a large economic loss which cannot be restored; or serious loss of reputation caused by revealing of sensitive and offending information.	Violation of law which results in minor penalty or fine; or a large economic loss which cannot be restored; or serious loss of reputation that will influence trust and respect for a long time.
Catastrophic	Death or permanent reduction of health; or considerable economic loss which cannot be restored; or serious loss of reputation which permanently influences life, health, and economy.	Serious violation of law which results in penalty or fine; or considerable economic loss which cannot be restored; or serious loss of reputation which is devastating for trust and respect.

Qualitative values for Risk level

Risk level	
Low	Acceptable risk. The service can be used with the identified threats, but the threats must be observed to discover changes that could increase the risk level.
Medium	The risk can be acceptable for this service, but each threat must be further inspected and the development of the risk must be monitored on a regular basis, with a following consideration whether necessary measures have to be implemented.
High	Not acceptable risk. Can not start using the service before risk reducing treatment has been implemented.

Definition of Risk Matrix

Consequence → / Likelihood ↓	Small	Moderate	Severe	Catastrophic
Low	Low	Low	Low	Medium
Moderate	Low	Medium	Medium	High
High	Low	Medium	High	High
Very high	Medium	High	High	High

Threat identification

- Method: Brainstorming
  - System architect, system developers, network expert + RA leader
  - Several meetings in a period of 2 months
- Approx. 30 threats

Threat table layout

ID	Threat, unwanted incident	Cause	Likelihood	Consequence	Risk	Comments, e.g. security measures

Risk Analysis

For each identified threat:

- Likelihood
- Consequence

Result of the Snow RA

Consequence → / Likelihood ↓	Small	Moderate	Severe	Catastrophic
Low	a7a	a2, a3a, a4, a5, a6b, a7b, i2, i3a, i3b	g2, c2a, c2b, c3, c4, c5, a1a, a1b, i1a, i1b	
Moderate	a6a		c1	
High		a3b		
Very high				

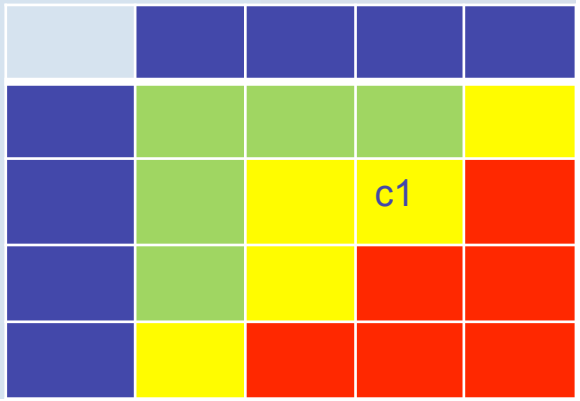
Identified threats

c1: Sensitive (person identifiable) information is extracted from the EHR and presented by the surveillance system.

Consequence: Severe

Likelihood: Moderate

→ Medium risk



Identified threats

a3b: Increased load on the local systems at the GP office, and correspondingly decreased responsiveness, caused by features in the surveillance system.

Consequence: Moderate

Likelihood: High

→ Medium risk

Identified threats

Low risk, but *Severe* consequence

g2: Fake software modules can be installed on the surveillance system's servers or in the GP's local systems.

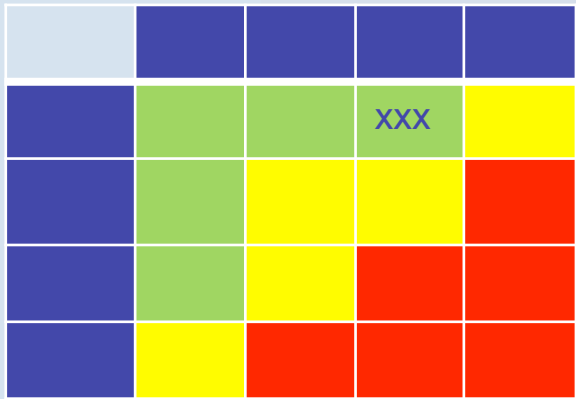
Identified threats (Confidentiality)

Low risk, but *Severe* consequence

c2a: Sensitive information from the GP's EHR is revealed to unauthorised persons by fake processes which are able to extract sensitive information from the EHR.

c2b: Sensitive information from the GP's EHR is revealed to unauthorised persons because errors in the surveillance software make it possible to extract sensitive information from the EHR.

c3: Sensitive information is exposed during transfer because of wiretapping, unauthorised persons "listening in" to the communication.

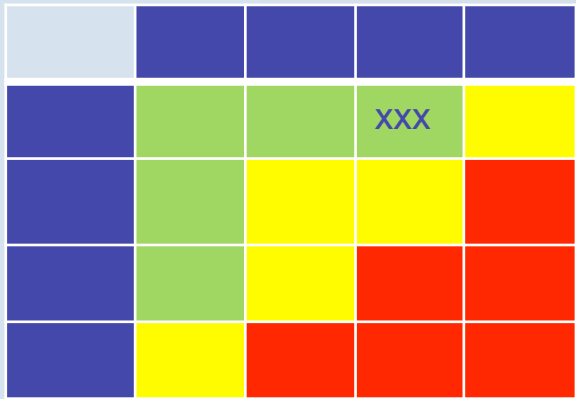


Identified threats (Confidentiality, cont.)

Low risk, but *Severe* consequence

c4: The GP *intentionally* performs a copy-paste operation from the EHR into a message which is submitted to a receiver.

c5: Delivery of information from GP, caused by an *unintentional* copy-paste, or by sending a message to a wrong receiver address.

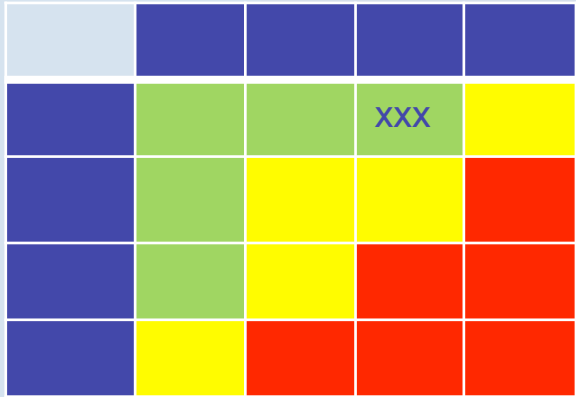


Identified threats (Availability)

Low risk, but *Severe* consequence

a1a: The surveillance system crashes the local EHR server, resulting in a disk crash and destroyed data.

a1b: The surveillance system crashes the local EHR server, causing the EHR system to be unavailable for a period of time.

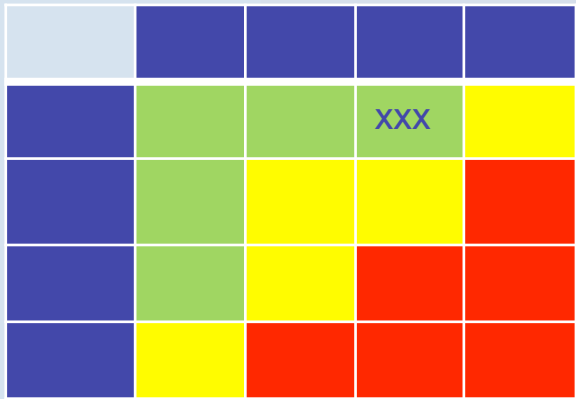


Identified threats (Integrity)

Low risk, but *Severe* consequence

i1a: Malicious software in the surveillance system causes modification of data and relations in the local EHR system, resulting in wrong patient treatment.

i1b: SW errors in the surveillance system causes modification of data and relations in the local EHR system, resulting in wrong patient treatment.



Conclusion

Benefits to the Snow system from RA:

- Information security incorporated from the early design stage
  - Threats → system requirements
  - Design solutions to avoid the threats

Further RA work:

- Repeat/revise the RA at later stage(s) in the system development process


Thank you