02244 Logic for Security
Project on Information Flow

- Hand-out: March 21, 2022
- Hand-in: via DTU Learn until May 9, 2022 **noon**
- We allow to work and hand-in in groups of up to 3 students.

  Each report must indicate which students are part of the group.

  The reports must be divided into sections, and each section must have one group member designated as responsible. This should reflect a fair distribution in report writing among the group members.
- The report must indicate which resources have been used to perform the work. This includes text books, research papers, information found on the web, detailed suggestions from teachers, and results of discussions or cooperation with other students.
- Page Limit: 15 pages (you may submit program files as attachments)
- Presentation: In the meeting on May 9, we ask groups to present the programs they have designed, so we can discuss the different solutions, common mistakes, and insights gained.

The Setting

In the pandamic crisis since 2020, several IT solutions have been developed for management of testing, vaccination, and the documentation thereof. Of course, the data being stored include personal information, in particular health care information. While one may want to give an individual the ability to prove their vaccination status, we do not for instance want that anybody can see the vaccination status of everybody.

Pretend that you are working in a software company that wants to design a new software solution for pandemic crises that benefits from past experience, and tries to improve now that we have time to reconsider designs. To be able to convince the Danish government (or even the European commission), the plan is to make a prototype concept which is a convincing concept with a demonstrator tool, so that the company gets awarded a contract for developing the system in full.

To be successful, one must convince the government that one has a state-of-the-art concept for handling the personal and health-related informations of the people in a suitable way. In particular it must be ensured that access to this information (in term of reading and/or writing) is limited to people who have a legitimate reason to access it, as defined by a policy. It must be formally verified that the system has no software bugs that would leak information or allow improper modification of data.

You are part of a small task force of 1-3 researchers that shall develop a demonstrator for such a system and to describe and motivate the design choices.

The Choice of Methods

Your manager has signed you up for a course on Logic for Security where you will learn in the coming weeks the following three approaches on formal verification of secure information flow:

- D. E. Denning, P. J. Denning: *Certification of Programs for Secure Information Flow*, Communications of the ACM (vol 20 no 7 pp 504-513), ACM Press, 1977.

- D. Volpano, C. Smith, C. Irvine: *A sound type system for Secure Information Flow*, Journal of Computer Security (vol 4 no 3 pp 167-197), IOS Press,1996.
- A. C. Myers, B. Liskov: *A Decentralized Model for Information Flow Control*, ACM Symposium on Operating Systems Principles (pp 129-142), ACM Press, 1997.

Your manager is convinced that the solution must be based on elements presented in the above papers and that you *must not* develop any alternative methods for information flow from scratch. In fact, you are expected to choose or combine techniques suitable for your approach, motivating your choices and discuss them in the course on Logic for Security.

The Demonstrator

Your manager expects you to start with a rather simple design and enlarge it as you go. It is of course not expected that the demonstrator covers the entire IT-system of a hospital, but only a few typical situations in a hospital. It is much more important that these few things work well in the demonstrator and are formally verified than a huge ambitious but incomplete study. An agile approach where a modest solution is subsequently improved is likely to be a good idea.

Your manager suggests that you consider a facility for testing and vaccination and the support the following operations:

- Patients can book online appointments for tests and vaccinations.
- The patients can be tested, the facility evaluates the test and enters the result for that particular patient into a national/European database.
- Similarly, vaccination can be applied to a patient, and the vaccination is entered into the database for that patient.
- Patients can retrieve their result or vaccination certificate from the database.
- The public can get from the database some statistical information, e.g., number of infections within the past seven days.

What to develop (and what not): Actually, of main interest is the core software that the facility is running, i.e., where data are entered into, and retrieved from, a database, and the information flow labels on these informations. You do not need to write user/web interfaces, or authentication mechanisms like MitID (we have already done that! :-) Also you do not need to write an information flow analyzer, but you can well do the information flow analysis manually.