Smart home intrusion detection using network intrusion detection techniques
Interim Presentation Log
Manuel Munoz

The most relevant conclusion of the interim presentation, is that the topic is too broad. Right now it is comprised of 3 subtopics. First, intrusion detection using network intrusion machine learning techniques. Second, building a smart home system that is extensible, that is, new sensors and actuators can be easily added. And lastly, the need of not having the privacy-invading sensors turned on all the time, just when they are most needed.

We need to focus on just one topic. The central motivating issue of the thesis should addressing reducing false positives, without focusing on the privacy factor of turning on and off the different sensors or being able to add sensors on runtime. Moreover, it could be said that false positives can cause privacy concerns, and reduced cost is a side benefit. Another side benefit that could be argued at the end, is that the algorithms will deal with extensible data, but is not one of the objectives. Therefore, one of the suggestions is to make the set-up fixed, but aim for the system to be robust. That is, in the context of change the algorithms should work.

Additionally, from the other two other topics the feedback is that having sensors turning on and off may not be useful. The user makes a trade-off between privacy and security. Furthermore, this should be modeled as a non-functional requirements.

There were also suggestions for the scenarios. They should focus on recognizing between good and bad guys, on similar situations. Also, a scenario of unusual behavior where for example a cleaning person forgets to turn off a light. There a soft alarm should be triggered.

One of the biggest suggestions is that several things need to be modeled from the start. For example, the threat and intrusions should be modeled in the analysis object model. Also, do a correct distinction between Entiy, Boundary, and Control objects. This distinction is difficult because boundary objects are usually user interface elements, making sensors and actuators also boundary objects.
Furthermore, there is and advantage to model intrusions. The actions taken should depend on the cause of the alarm. For example, sound an alarm or investigate further. For that a taxonomy of alarms may be needed.
From the use case diagram, sensors and actuators should be modeled as actors as well.
On the analysis object model some entities need to be added, for example, the guardian. Also, high level categories of sensors should be shown in the analysis object model, as well as the alert types.

For the design phase, the taxonomy defined on analysis, must be further developed, for example the threat taxonomy from the analysis is mapped onto the state machine.
Some sensors only are defined only on the system design phase, for example the camera. Which will later be used as different data source to disambiguate an intrusion has happened or not
The use of the blackboard is a system design decision, as it is an architectural style. The state changes is a hypothesis on the blackboard that should be evaluated by the knowledge sources.
Using OpenHAB is also regarded as system design decision.
Focus on at least 2 intrusion detection algorithms (naive; GA; +1). The third one can be the work by Roy Maxion on statistical anomalies. Interesting as it does not need training.
The strategy pattern can also be integrated by having different algorithms and comparing them, evaluating in runtime.