Explainable security

Jan Willemson
janwil@cyber.ee
AI is getting better at everything
... but it is also hard to understand
Security measures are not always easy to explain either
Security measures are not always easy to explain either

E-voters can change their votes while paper voters can’t. This is not fair!
Security measures are not always easy to explain either

Laupäevast läheb mobiiliga maksmine palju tüljakamaks

Alvar Pau
@alvarpau
Can we have easy to explain security measures?

- What is a good measure of explainability?
- Is it true that people are more likely to obey security requirements they understand?
- What are reasonable explainability-security-performance trade-offs?
- Can we have explainability as a non-functional requirement in the system development process?
- How would some of our present systems differ if they would emphasise explainability over, say, performance?
- What are the links between explainability and usability?

Your task is to read through recent papers on the topic (3-4 in total) and write a report.

Some social science interest/background feels useful, but not strictly necessary.