Open your mind. LUT.

Lappeenranta University of Technology

Nothing to hide: Chapters 2-3

CT60A7001 - Critical Thinking and argumentation in Software Engineering

Discussion day 1
Artem Khvatov

The Nothing-to-hide argument

- Everybody has something to hide
- Even if you aren't trying to hide some insensitive information, it doesn't mean you want everyone to know it
- Part of the problem is not recognizing the problem
  - Program is said to be only interested in information regarding security
  - If you have nothing to hide then you don't need to worry about it etc.
- Another problem is how privacy is given low value
  - The security program is considered to outweight the sacrifice of privacy
- Privacy is seen as secrecy – a right to hide things, but the problem is bigger than exposing some secrets to government

The Nothing-to-hide argument

- Violation of privacy only being recognized upon harm
- Privacy is violated only upon revealing something embarassing or discrediting
- Privacy harm distanced from other types of harm, because “it lacks blood and death”
- Problem is however not the singular harm caused by a single violation, but overall loss of ability to keeping your private information secure
  - Who want's to reveal everything to everyone?
  - How to know what information is being collect?
  - How to know your information is not misused?
  - How to know who can view your information?

The Nothing-to-hide argument

- These questions lead to certain issues caused by Nothing-to-hide argument
- Even if collected information doesn't harm you in any way, there is no way to know it can harm you in future
- Several ways the collection of information can harm individual are often ignored, for example Kafkaesque information processing problems
  - Aggregation (fusion of small innocent bits of data into sensitive information)
  - Exclusion (preventing people from accessing and correcting information)
  - Secondary use (use of information for unrelated purposes without consent)
  - Distortion (getting wrong picture, because of missing information bits)

The All-or-nothing fallacy

- The core problem of All-or-nothing fallacy is how it views privacy and security as exclusive properties
- Because of this privacy is often being sacrificed
- Severely unbalanced towards security, as it is viewed as more important
- The problem is that the sacrifice of privacy doesn't necessarily mean gains in security
- The view that gain in security has to be a loss in privacy itself is flawed
- Not all security issues are privacy invasive

The All-or-nothing fallacy

- Ironically people feel more secure the more government invades their privacy
  - This however is often just an illusion
  - Actual security is not necessarily improved at all
- The solution to this problem is to focus on methods that don't invade privacy
  - If there has to be invasion of privacy, then the tradeoff has to be justified
  - Often however this is viewed as all-or-nothing tradeoff between security or privacy
- Solving this problem requires to first recognize that protecting privacy does not negate security measure entirely

Questions

- How to measure the benefits of invading privacy?
  - How to know how many terror attacks are prevented by sacrificing privacy of thousands?
  - Is it a justified tradeoff?