


4.3 Attacker Models and Assumption Coverage

Felix Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE), Frederik Armknecht (Universität Mannheim, DE)

License  Creative Commons BY 3.0 Unported license
© Felix Freiling, Frederik Armknecht

In his seminal paper on “failure mode assumptions and assumption coverage” [1], David Powell defines several central concepts:

1. The notion of *failure mode assertions*, i.e., precise statements about the way in which certain components may fail in the time domain and the value domain.
2. The *failure mode implication graph*, i.e., a lattice induced by the combination of failure modes defining the partial order between different composed failure modes.
3. The notion of *assumption coverage*, i.e., the probability that the assertion defining the assumed behavior of a component proves to be true in practice conditioned by the fact that the component has failed [1, p. 391].

The goal of this discussion session was to reflect on the similarities and differences between safety and security regarding attacker assumptions and assumption coverage and to ask whether any related work and concepts exist. Safety was understood here as the area of fault-tolerance and dependability, whereas security was understood as the area of cryptography. The connection to the title of this Dagstuhl seminar was the fact, that one of the biggest failures in security appears to be the fact that we do not learn sufficiently from other areas.

Regarding the concept of attacker assumptions, our observation was that in safety attacker assumptions are usually fixed for a specific scenario and in this scenario often empirically measurable. Examples are failure rates of components or maximum frequency of bitflips on communication lines or in memory. The mechanism, with which a component attempts to tolerate these problems, has no influence on the assumption coverage.

In security, the attacker assumption is usually determined by a domain expert and must be regularly checked whether it is still correct. It can even change spontaneously. In circumstances where this is expected to happen, issues of *risk management* arise. Furthermore, security mechanisms can have an effect on attacker behavior:

- either a strong mechanism deters attackers and makes the system uninteresting compared to others,
- or a weak mechanism is circumvented easily with minimal effort.

In safety we have concepts like *graceful degradation* and *stabilization*. On the one hand, graceful degradation means that the level of violation of specification is proportional to the strength of failure behavior. On the other hand, stabilization refers to a temporary violation of a safety property if attacker assumption is violated, and a return to safety property when attacker assumption is satisfied.

In security, the attacker assumption is usually a worst-case attacker assumption. Intermediate levels of attackers are unusual. Also switching between different security mechanisms is unusual and it is unclear on what basis the switch should occur since many violations of confidentiality and integrity are undetectable.

In the discussion, people from security admitted that worst-case assumptions usually are preferred, but often also weaker assumptions are used, so the cryptography community does not really live up to this claim of always choosing worst-case assumptions.

It was also mentioned that *testing* has strong similarities to transient attacks that try to throw a single machine off the tracks, and that stabilization has similarities to the mechanisms used to tolerate denial-of-service attacks.

References

- 1 David Powell. Failure mode assumptions and assumption coverage. In *Digest of Papers: FTCS-22, The Twenty-Second Annual International Symposium on Fault-Tolerant Computing, Boston, Massachusetts, USA, July 8-10, 1992*, pages 386–395, 1992.

4.4 Values in Computing – a Short Talk

Lucy Hunt (Lancaster University, GB)

License © Creative Commons BY 3.0 Unported license
© Lucy Hunt

Joint work of Emily Winter, Stephen Forshaw, Lucy Hunt, Maria Angela Ferrario

Main reference Emily Winter, Stephen Forshaw, Lucy Hunt, Maria Angela Ferrario: “Towards a systematic study of values in SE: tools for industry and education”, in Proc. of the 41st International Conference on Software Engineering: New Ideas and Emerging Results, ICSE (NIER) 2019, Montreal, QC, Canada, May 29-31, 2019, pp. 61–64, IEEE / ACM, 2019.

URL <https://doi.org/10.1109/ICSE-NIER.2019.00024>

Values in Computing (ViC) is about understanding how human values influence software production and transforming the way values are considered in software industry practices, policy making and education. With the increasing number of high impact technology breaches and failures, we need computing professionals equipped to understand what human values are and what social responsibility means. To this end, we need to help create more resilient, secure and less vulnerable software systems that are mindful of the wider ethical, social and human impact of what their technology does or could do. ViC has a body of research establishing a framework for the systematic investigation of human values in software production and a website to disseminate our work (www.valuesincomputing.org).

How can software (security) incident story-telling be used to improve SE industry and education practices?

4.5 DRM and Security – A Big Failure?

Stefan Katzenbeisser (Universität Passau, DE)

License © Creative Commons BY 3.0 Unported license
© Stefan Katzenbeisser

In the talk we discuss the evolution of Digital Rights Management techniques, which were proposed to secure online content. The key idea was to encrypt content and transmit the encryption key in a special license. The failure of DRM can be tracked down to technical issues (such as the absence of trusted hardware at that time), changes in the business model (such as the uprising of flatrate streaming media) and usability problems. Media security tried to fill this gap by marking distributed media invisibly. Still, the fundamental different nature of analog signals led to numerous problems (such as robustness issues and conflicts in dispute resolution). Nevertheless, the techniques developed in the area of media security nowadays play a significant role in the construction of covert channels.