Compositionality of Secure Information Flow

Catuscia Palamidessi

INRIA and LIX, École Polytechnique, Palaiseau, France

One of the concerns in the use of computer systems is to avoid the leakage of confidential information through public outputs. Ideally we would like systems to be completely secure, but in practice this goal is often impossible to achieve. Therefore it is important to have a way to quantify the amount of leakage, so to be able to assess that a system is better than another, although they may both be insecure. Recently there have been various proposals for quantitative approaches. Among these, there is a rather natural one which is based on the Bayes risk, namely (the converse of) the probability of guessing the right value of the secret, once we have observed the output [1]. The main other quantitative approaches are those based on Information Theory: intuitively indeed the information leakage can be thought of as the certainty we gain about the secret by observing the output, and the (un)certainty of a random variable is represented by its *entropy*. The information-theoretic approaches, in the early proposals (see for instance [2–4]), were based on the most common notion of entropy, namely Shannon entropy. However Smith has argued in [5] that Shannon entropy, due to its averaging nature, is not very suitable to represent the vulnerability of a system, and he has proposed to use Rényi's min entropy [6] instead. In the same paper, Smith has also shown that the approach based on Rényi's min entropy is equivalent to the one based on the Bayes risk.

In this work, which continues a line of research initiated in [7], we consider a formalism for the specification of systems composed by concurrent and probabilistic processes, and we investigate "safe constructs", namely constructs which do not increase the vulnerability.

References

1. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: On the Bayes risk in information-hiding protocols. Journal of Computer Security **16**(5) (2008) 531–571
2. Clark, D., Hunt, S., Malacaria, P.: Quantitative information flow, relations and polymorphic types. J. of Logic and Computation **18**(2) (2005) 181–199
3. Zhu, Y., Bettati, R.: Anonymity vs. information leakage in anonymity systems. In: Proc. of ICDCS, IEEE (2005) 514–524
4. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: Anonymity protocols as noisy channels. Inf. and Comp. **206**(2–4) (2008) 378–401
5. Smith, G.: On the foundations of quantitative information flow. In: Proc. of FOSSACS. Volume 5504 of LNCS., Springer (2009) 288–302
6. Rényi, A.: On Measures of Entropy and Information. In: Proc. of the 4th Berkeley Symposium on Mathematics, Statistics, and Probability. (1960) 547–561
7. Braun, C., Chatzikokolakis, K., Palamidessi, C.: Compositional methods for information-hiding. In: Proc. of FOSSACS. Volume 4962 of LNCS., Springer (2008) 443–457