Entropy and Attack Models in Information Flow
(Invited Talk)

Mário S. Alvim[1], Miguel E. Andrés[2], and Catuscia Palamidessi[1]

[1] INRIA and LIX, École Polytechnique, Palaiseau, France
[2] University of Nijmegen, The Netherlands

In recent years, there has been a growing interest in considering the quantitative aspects of Information Flow, partly because often the a priori knowledge of the secret information can be represented by a probability distribution, and partly because the mechanisms to protect the information may use randomization to obfuscate the relation between the secrets and the observables.

Several works in literature use an Information Theoretic approach to model the problem and define the leakage in a quantitative way, see for example [17,4,9,10,13,12,2]. The idea is that the system is seen as a *channel*. The input represents the secret, the output represents the observable, and the correlation between the input and output (*mutual information*) represents the information leakage. The worst case leakage corresponds then to the *capacity* of the channel, which is by definition the maximum mutual information that can be obtained by varying the input distribution.

In the works mentioned above, the notion of mutual information is based on *Shannon entropy*, which (because of its mathematical properties) is the most established measure of uncertainty. From the security point of view, this measure corresponds to a particular model of attack and a particular way of estimating the security threat (vulnerability of the secret). Other notions have been considered, and argued to be more appropriate for security in certain scenarios. These include: *Rényi min-entropy* [1,16], *Bayes risk* [3], *guessing entropy* [11], and *marginal guesswork* [14]. Köpf and Basin discuss the relation between brute-force guessing attacks and entropy in [8], in the context of information flow induced by a deterministic program, and define the information leakage as difference between the input entropy and the conditional one, namely the entropy based on the a priori input distribution, and the entropy of the a posteriori distribution (i.e. after observing teh output), respectively. One of their main results is that, in their framework, the notion of leakage under the various notions of attacks considered in their paper is always non-negative.

In this talk, we extend the analysis of Köpf and Basin to the probabilistic scenario, and we consider also other notions of entropy, including the family of entropies proposed by Rényi [15]. We argue that in the probabilistic case the notion of information leakage needs to be revised. In fact, when the same secret can give different observables (according to a probability distribution), the difference between a priori and a posteriori entropy may be negative. This is due to the fact that the notion of entropy uses the probability distribution in two different ways: for averaging and for representing the belief of the attacker. While the leakage should depend on the difference induced by the belief change

due to the observation, the averaging probability should remain the same. (A similar concern has also inspired the works of [5] and [7].) In order to avoid the unnatural consequence of a negative leakage, we propose to base the notion of leakage directly on the (more primitive) notion of mutual information. We consider some cases of entropy, in particular the Rényi's entropies, for which the corresponding notion of mutual information has been investigated in [6], and we show that in this way the property of non-negativeness is ensured.

References

1. Cachin, C.: Entropy Measures and Unconditional Security in Cryptography. PhD thesis (1997)
2. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: Anonymity protocols as noisy channels. Inf. and Comp. 206(2-4), 378–401 (2008)
3. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: On the Bayes risk in information-hiding protocols. Journal of Computer Security 16(5), 531–571 (2008)
4. Clark, D., Hunt, S., Malacaria, P.: Quantitative information flow, relations and polymorphic types. J. of Logic and Comp. 18(2), 181–199 (2005)
5. Clarkson, M.R., Myers, A.C., Schneider, F.B.: Belief in information flow. Journal of Computer Security 17(5), 655–701 (2009)
6. Csiszár, I.: Generalized cutoff rates and Rényi's information measures. Transactions on Information Theory 41(1), 26–34 (1995)
7. Hamadou, S., Sassone, V., Palamidessi, C.: Reconciling belief and vulnerability in information flow. In: Proc. of the IEEE Symposium on Security and Privacy. IEEE, Los Alamitos (to appear, 2010)
8. Köpf, B., Basin, D.A.: An information-theoretic model for adaptive side-channel attacks. In: Proc. of CCS, pp. 286–296. ACM, New York (2007)
9. Malacaria, P.: Assessing security threats of looping constructs. In: Proc. of POPL, pp. 225–235. ACM, New York (2007)
10. Malacaria, P., Chen, H.: Lagrange multipliers and maximum information leakage in different observational models. In: Proc. of PLAS, pp. 135–146. ACM, New York (2008)
11. Massey: Guessing and entropy. In: Proceedings of the IEEE International Symposium on Information Theory, p. 204. IEEE, Los Alamitos (1994)
12. Moskowitz, I.S., Newman, R.E., Crepeau, D.P., Miller, A.R.: Covert channels and anonymizing networks. In: Proc. of PES, pp. 79–88. ACM, New York (2003)
13. Moskowitz, I.S., Newman, R.E., Syverson, P.F.: Quasi-anonymous channels. In: Proc. of CNIS, pp. 126–131. IASTED (2003)
14. Pliam, J.O.: On the incomparability of entropy and marginal guesswork in brute-force attacks. In: Roy, B., Okamoto, E. (eds.) INDOCRYPT 2000. LNCS, vol. 1977, pp. 67–79. Springer, Heidelberg (2000)
15. Rényi, A.: On Measures of Entropy and Information. In: Proc. of the 4th Berkeley Symposium on Mathematics, Statistics, and Probability, pp. 547–561 (1961)
16. Smith, G.: On the foundations of quantitative information flow. In: de Alfaro, L. (ed.) FOSSACS 2009. LNCS, vol. 5504, pp. 288–302. Springer, Heidelberg (2009)
17. Zhu, Y., Bettati, R.: Anonymity vs. information leakage in anonymity systems. In: Proc. of ICDCS, pp. 514–524. IEEE, Los Alamitos (2005)