

IT-Universitetet

| København

Carsten Schürmann

++45.72.18.52.82

carsten@itu.dk

To the
PhD School
IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S

Copenhagen, May 15, 2014

Preliminary Evaluation Report of Fabrizio Biondi's dissertation

We evaluated the dissertation, submitted by Fabrizio Biondi is cumulative and consists of five individual papers. The first chapter of the thesis motivates the organization of the dissertation. The second chapter introduces the prerequisite mathematics, necessary to understand the technical developments in the later parts of this thesis. Section 3 then introduces the state of the art and discusses related work. The technical development of the dissertation includes Chapter 4 - Chapter 7.

The dissertation core contribution is about quantifying and measuring the information leakage in systems modeled as Markov chains. The "statement of the thesis", presents the use of Markov chains in opposition to other models used in the past (in particular, channel matrices) and argues about the advantages of this approach. This sounds like an overstatement: We don't think that the use of Markov chains is a breakthrough with respect to previous models, but, rather, a generalisation: on each state, the behavior of the system could be equivalently described as a channel matrix, and also the leakage measure on each state is defined in the way it has been defined in the literature. Hence the whole model corresponds to a Markovian sequence of channel matrices, and we would recommend to reformulate the statement in this sense. This said, the thesis contains many novel contributions: in particular, the investigation of the interaction between the system and the attacker, the definition of the leakage of the whole system, and the development of methods and tools for computing it. We comment on each of the chapters in turn.

Chapter 1 This chapter consists of the introduction. After explaining the motivations for studying information leakage, and giving a brief summary of the research done in the field so far, the author presents the "statement of the thesis". Then, he proceed to

describe the contributions of his thesis, and the papers on which it is based. Page 2: Attackers that are ordered according to one of the measures will be ordered according to all of them [56]. Furthermore, the ordering is a complete lattice, known as the Lattice of Information [52].

Chapter 2 This chapter recalls some preliminary notions that will be used in the rest of the thesis: Discrete Probability, Markov chains and Markov decision processes, and information theory.

Chapter 3 This chapter is dedicated to an overview of the literature on information leakage. In particular, the authors focus on the information-theoretic approaches which have been proposed as a way to quantify leakage, notably those based on Shannon entropy and Rényi min-entropy. This chapter also recalls the related notion of Bayes risk, and the recently proposed notion of g -leakage. Finally, it illustrates the typical notion of adversary in terms of its probabilistic side knowledge. The author shows a good and systematic knowledge of the state of the art.

Chapter 4 This chapter contains the first novel contributions of the thesis: the model of process and attacker based on Markov decision processes, and how to obtain a Markov chain from their interaction. Then, it proposed a notion of entropy for the Markov chain, and a definition of information flow and capacity for the whole system. In particular, it focuses on the issue of non-termination, and proposes some methods to detect non-termination and, more generally, unsafe behavior. This chapter also discusses a method to find the maximal-leakage implementation among those which satisfy a given implementation. These results are interesting and original. As far as we know, the work of the author (and of the coauthors of the papers on which this chapter is based) is the first to investigate and extend the information-theoretic notion of leakage to the case of interactive systems described as Markov chains.

Chapter 5 This chapter extends the work from Chapter 4 to cover non-terminating processes, particularly those with infinite inputs and outputs. The rate of leakage is introduced to give useful results about programs over time.

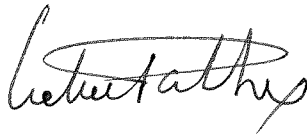
Chapter 6 This chapter presents the QUAIL tool, which implements the theory from Chapter 4. This tool analyses programs written in a simple while loop language and calculates their leakage. It is a very well developed piece of work and is certainly one of the best information leakage analysis tools in the world. It helps to justify the theoretical work by showing that it is useful in practice.

Chapter 7 This chapter represents some large case studies using the QUAIL tool. All of our positive comments from Chapter 6 also apply to this chapter and these larger case studies. These are substantial case studies which produce interesting results. In particular the comparison of Onion Routing, Tor and Crowds produces very good results. We would however like the code for these examples to be made available.

Overall Evaluation The dissertation addresses interesting and timely problems in information leakage and includes advanced techniques and tools to quantify and compute such leakage. Fabrizio gave a very clear and confident presentation and he handled questions excellently. In addition, he demonstrated good control over the broader subject area. His dissertation work was meticulously executed, and therefore, we recommend that he be awarded the degree of Ph.D.



Tom Chothia
(Lecturer)



Catuscia Palamidessi
(Professor)



Carsten Schürmann
(Associate Professor)