Bayesian Inference to Evaluate Information Leakage in Complex Scenarios

Carmela Troncoso
Galician R&D Center in Advanced Telecommunications (Gradiant)
CITEXVI, Campus Universitario
Vigo, Spain
ctroncoso@gradiant.org

ABSTRACT

Common security evaluation methods require the estimation of the likelihood of a hidden state given an observation of the system. For instance: identifying the type of tampering on an image given the tampered file, identifying communication partner given an anonymous channel trace, identifying the location from where a service has been accessed given an obfuscated version of this location. In this talk we explore the suitability of Bayesian Inference techniques, specifically Markov Chain Monte Carlo methods, to evaluate information leakage in complex scenarios.

Using anonymity systems, in particular mix networks, as case study we show that casting problems in the context of Bayesian inference provides an appropriate framework to evaluate security properties (e.g., traceability of messages) in complex constraints.

We present a generative probabilistic model of mix network architectures that incorporates a number of attack techniques in the trace analysis literature. We use the model to build a Markov Chain Monte Carlo inference engine based on the Metropolis-Hastings algorithm that calculates the probabilities of who is talking to whom given an observation of network traces. Finally, we briefly overview other Bayesian techniques, such as Gibbs sampling and particle filtering, that are useful to tackle other security problems, like user profiling, or to consider dynamic behaviour.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*

General Terms

Security, Measurement, Theory

IH&MMSec'13, June 17–19, 2013, Montpellier, France.
ACM 978-1-4503-2081-8/13/06.

Keywords

Bayesian inference, Monte Carlo, Information leakage

Bio

Carmela Troncoso was born on September 17th 1982 in Vigo, Spain. She received the Master's degree in Telecommunications Engineering from the University of Vigo, Spain, in May 2006. She joined the COSIC research group at the Katholieke Universiteit Leuven, Belgium as a PhD student in October 2006 obtaining her doctoral degree in April 2011. Her thesis *Design and Analysis methods for Privacy Technologies* received the European Research Consortium for Informatics and Mathematics WG Security and Trust Management Best Ph.D. Thesis Award.

Carmela has been a research visitor at numerous worldwide known security groups amongst them Microsoft Research Cambridge, the Hatswich Research group at the University of Illinois at Urbana-Champaign, or the LCA1 lab at the École Polytechnique Féderale de Laussane. She is a co-author of more than 25 publications in peer-reviewed international conferences and journals. She has been program chair of the Hot Topics in Privacy Enhancing Technologies Workshop (HotPETs) in 2010 and 2011, and General Chair of the Privacy Enhancing Technologies Symposium in 2012. She has also served on more than 10 program committees of international conferences, and reviewed articles for numerous international journals. Since October 2012 she is a postdoctoral research at Gradiant in the framework of the LIFTGATE project.