A CONCEPT PAPER FOR CHECKING PROBABILISTIC DENIABILITY

CS EVE Group 207

April 19, 2017

1 Executive Summary(Abstract)

We use the probabilistic deniability to analyze the Crowds system for anonymous Web browsing. This case study demonstrates how probabilistic deniability techniques can be used to formally analyze security properties of a peer-to-peer group communication system based on random message routing among members. The behavior of group members and the adversary is modeled as a discrete-time Markov chain, and the desired security properties are expressed as PCTL formulas.ur main result is a demonstration of how certain forms of probabilistic anonymity degrade when group size increases or random routing paths are rebuilt, assuming that the corrupt group members are able to identify and/or correlate multiple routing paths originating from the same sender.

2 Introduction

Formal analysis of security protocols is a well-established field. Model checking and theorem proving techniques have been extensively used to analyze secrecy, authentication and other security properties systems that employ cryptographic primitives such as public-key encryption, digital signatures, etc. Conventional formal analysis of security is mainly concerned with security against the so called Dolev-Yao attacks Many proposed systems for anonymous communication aim to provide strong, non-probabilistic anonymity guarantees. Non-probabilistic anonymity systems are amenable to formal analysis in the same non-deterministic Dolev-Yao model as used for verification of secrecy and authentication protocols.In this project, we use probabilistic model checking to analyze anonymity properties of a gossip-based system. Such systems fundamentally rely on probabilistic

message routing to guarantee anonymity. The first flaw was identified by the authors of

Crowds [RR98] and analyzed by Makhi [Mal01] and Wright et al. [WALS02] Previous research on probabilistic formal models for security focused on

1. Probabilistic characterization of non-interference, and

2. Process formalisms that aim to faithfully model probabilistic properties of cryptographic primitives. This paper attempts to directly model and analyze security properties based on discrete probabilities, as opposed to asymptotic probabilities in the conventional cryptographic sense. Our analysis method is applicable to other probabilistic anonymity systems such as free net and onion routing.

3 Problem Statement

The problem this project will tackle is to maintain the privacy of communicated data against passive eavesdroppers (A secret listener to private conversations). The key solution to the problem is by constructing a sender-deniable public key encryption scheme based on any trapdoor permutation. However, our scheme falls short of achieving the desired level of deniability.

4 Objectives

4.1 General Objectives

To analyze the anonymity properties of a crowds system using a probabilistic model checker (PRISM).

4.2 Specific Objectives

1. To prevent corrupt crowd members from linking multiple paths and using this information to infer the initiators identity, the Crowds paper suggests that paths should be static.
2. To formally specify properties of the crowd system to be checked using a temporal probabilistic PCTL(Probabilistic Computation Tree Logic) formulas.
3. To hide each users communication by routing them randomly within a crowd of similar users.

5 Scope

This case study demonstrates how probabilistic model checking techniques can be used to formally analyze security properties of a peer-to-peer group communication system based on random message routing among members.

6 Research Significance

Our main result is a demonstration of how certain forms of probabilistic anonymity degrade when group size increases or random routing paths are rebuilt.

7 Literature Review

1. **Markov Chain Model Checking.**
   We model the probabilistic behavior of a peer-to-peer communication system as a discrete-time Markov chain (DTMC), which is a standard approach in probabilistic verification

2. **PRISM Model Checker**
   The automated analyses described in this paper were performed using PRISM, a probabilistic model checker developed by Kwiatkowska et al.. The tool supports both discrete- and continuous-time Markov chains, and Markov decision processes. We model probabilistic peer-to-peer communication systems such as Crowds simply as discrete-time Markov chains, and formalize their properties in PCTL.

3. **Anonymity properties of Crowds.**
   The Crowds paper describes several degrees of anonymity that may be provided by a communication system. Without using anonymizing techniques, none of the following properties are guaranteed on the Web since browser requests contain information about their source and destination in the clear i.e. Beyond suspicion, Probable innocence, Possible innocence.

8 Conclusion

Probabilistic deniability is a well-established technique for verification of hardware and concurrent protocols. The main contribution of this paper is to hint how it can be applied to the analysis of security properties based on discrete probabilities. We analyzed anonymity properties of the Crowds system, a real-world protocol for anonymous Web browsing. Anonymity in Crowds is based on constructing a random routing path to the destination through a group of members, some of whom may be corrupt. The path construction protocol is purely probabilistic, therefore, we modeled it as a discrete time Markov chain, without introducing non-determinism and thus avoiding the need for Markov decision processes.

References

[1] R. Alur and T. Henzinger *Reactive modules. In Proc. 11th Annual IEEE Symposium on Logic in Computer Science (LICS), pages 207 218* 1996.

[2] C. Baier *On algorithmic verification methods for probabilistic systems* 1998. Fakultat fur Mathematik and Informatik, Universitat Mannheim.

[3] . Bianco and L. de Alfaro.*Model checking of probabilistic and nondeterministic systems. In Proc. Foundations of Software Technology and Theoretical Computer Science (FST and TCS), volume 1026 of LNCS, pages 499513. Springer-Verlag* 1995