Limited use cryptographic tokens in securing cloud servers

Gautam Kumar, Brent Lagesse
Computing and Software Systems
University of Washington Bothell
{gautamk,lagesse}@uw.edu

ABSTRACT

INTRODUCTION

Leslie Lamport [1] was first to propose the use of hash chains in his paper on a method for secure password authentication over an insecure medium. In this paper we try to use the limited use property of hash chains to secure configuration information on ephemeral cloud servers.

BACKGROUND

Cryptographic hash function [3]

A cryptographic hash function is any one way function which meets the following requirements

- Preimage resistance
- Collision resistance
- Second Preimage resistance

A hash function has preimage resistance if given a hash value h it is computationally infeasible to find any message m such that $h = hash(k, m)$ where k is the hash key.

A hash function is collision resistant if, given two messages m_1 and m_2 it is hard to find a hash h such that $h = hash(k, m_1) = hash(k, m_2)$ where k is the hash key.

A hash function has second pre-image resistance if given a message m_1 it is computationally infeasible to find a different message m_2 such that $hash(k, m_1) = hash(k, m_2)$ where k is the hash key. The second pre-image resistance is a much harder property to achieve for hash functions. This property is closely related to the birthday problem [2].

Hash Chains

ARCHITECTURE

PERFORMANCE TESTING

FUTURE WORK

RELATED WORK

REFERENCES

[1] Leslie Lamport. Password authentication with insecure communication. 24(11):770–772.

[2] Lawrence M. Lesser. Exploring the birthday problem with spreadsheets. 92(5):407–411.

[3] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Bimal Roy and Willi Meier, editors, *Fast Software Encryption*, number 3017 in Lecture Notes in Computer Science, pages 371–388. Springer Berlin Heidelberg. DOI: 10.1007/978-3-540-25937-4_24.