Project Proposal: Securing Encryption Algorithms with Pre-image Disturbance

Betty Huang

October 29, 2009

Abstract

Since 2005, collision factors have been found for the SHA-1 algorithm. This paper aims to provide several mechanisms to improve the applicability of the algorithm for areas that are not able to adopt a new standard readily. Authors such as Yiqun Lisa Yin, Michael Szydlo, and various members of the National Institute of Standards and Technology have written about the possibilty of modifying the original input in order to reduce the likelihood of collisions/pre-image attacks, but none have tested extensively on how much the randomization would increase the efforts of decrpytion. I hope to be able to test a (likely simplified) version of the techniques against several sophisticated collision-based attacks.

1 Introduction

1.1 Purpose

Since the advent of the encryption algorithms, there have been numerous attempts to reverse engineer the process in order to return the original input. Thus, the response of NIST has been to develop stronger algorithms. The weaker, "obsolete" algorithm is then cycled out of use. However, the implementation of a stronger security standard may take years. However, there is a need for a method that can reduce the chances of breaking the encryption algorithm, without modifying the algorithm itself. This would not be as difficult to implement, and can secure the privacy of individuals while

the administrators switch to a newer algorithm. Thus, my project seeks to find out how "efficient" (ie. how much effort a collision attack would require) these modifications are.

1.2 Scope of Study

The field of study will be in encryption and cryptanalysis, mostly in Python/C. I hope to focus on the MD5 and the SHA family of encryption algorithms, and using tunneling and weight disturbance to analyze the effort required to find collisions pre- and post- message altering.

2 Review of Literature

Two articles have proven to be particularly useful in constructing an idea. Collision-Resistant usage of MD5 and SHA-1 via Message Preprocessing, by Yin and Szydlo, offers methods of implementing these preemptive techniques. Randomized Hashing for Digital Signatures by Quynh Dang also outlined the need for a security standard using pre-image processing techniques. There have also been several papers that detailed streamlined processes to break the MD5, but one in particular mentions the usage of tunnelling, which is a vast improvement over using differentials that required sufficient conditions (Wang et al.); instead of requiring effort values of pow(2,29), Klima's method on generating Points of Verifications (POVs), which are necessary to generate collisions. Klima's method is known as a multi-message modification method, which requires that each block individually in the MD5 hash would be considered in finding collisions.