RESEARCH PAPERS

RAYAT-BAHRA UNIVERSITY
Mohali

Cryptography & Network Security Hash Function Applications, Attacks and Advances: A Review

Arvind K. Sharma[1], Dr. S.K. Mittal[2]

(This paper explaining importance of hash functions, widely used in networking.)

Dr. S.K MITTAL
Ph.D,M.Tech (Computer Sc & Tech)
Dean R&D and Professor in Computer Sc & Engg

Proceedings of the Third International Conference on Inventive Systems and Control (ICISC 2019)
DVD Part Number: CFP19J06-DVD; ISBN: 978-1-5386-3949-8

Cryptography & Network Security Hash Function Applications, Attacks and Advances: A Review

Arvind K. Sharma[1], Dr.S.K. Mittal[2]

Department of Computer Applications (MMICT&BM)[1]
Maharishi Markandeshwar University, Mullana, Ambala (Haryana), India
University School of Engineering & Technology[2]
Rayat Bahra University, Sahibzada Ajit Singh Nagar (Punjab), India
Email: arvind.sharma@mmumullana.org[1], skmskm1@rediffmail.com[2]

Abstract: — Hash Functions have a distinct paramount significance in the sub domain of Networking like Network Security, Computer Security and Internet Security as compare to Symmetric and Public Key Encryption-Decryption Techniques. Major issues primarily which resolved by any hash algorithm are to managing the Integrity of Plaint-text Message(s) which are to be transmitting between communicating parties and to prove the Authenticity of Resources (Users/Machines), with digital signatures as well. Hash function also utilized for computing random secrect key of fixed length which further feeds to Symmetric and Public Key Cryptosystems in particular Key Management. Different level of security provided by different algorithms depending on how difficult is to break them. The most well-known hash algorithms are MD4, MD5, SHA, JH, Skein, Grøstl, Blake, Hamsi, Fugue, Crush, Whirlpool, Tav etc. In this paper we are discussing importance of hash functions, hash functions widely used in networking their application, literature and most importantly various Attacks applicable on hash functions and compression functions utilized by hash functions.

Keywords: *Algorithms; Compression Function, Cipher; Stream; Block; Confidentiality; Integity; Authentication; Server; Message-Digest, Message-Block, Non-repudation; Differential;*

I. Introduction

In Computer Networking particularly i.e., in interconnected environement 'Security & Privacy' means to preserve the Confidentiality, Integrity and Authenticity of plain-text messages as well as to manages the Accountability (i.e., to study the activities) and Authorization of resources, to be used. Security initializes with Authorization i.e. enterance to particular system premises commonly with the help of pre-specified credentials like 'Username' and 'Password'. Network Security consists of the Policies adopted or Rules specified by a Network Analysist, Administrator or Cyber Security Experts to prevent and track unauthorized access (i.e., with ACL (Access Lists), Logs, Firewalls) and modification in system and, denial of a computer network and network resources [45][46]. These secrets are distributed in a private manner in order to make Login successful afterwards (like with Certificates, Kerberos or Radius Servers) to Resources. If a user authorized to do something still, a firewall forces to access policies or rules such as what services are allowed to be accessed for that network user and to that user w.r.t. current location, as some services only to be accessed by authorized users in intranet not on internet. So these policies are okay to prevent unauthorized access to system, but this component may fails to check potentially harmful content such as computer Worms or Trojans being transmitted over the network. Anti-virus software or an Intrusion Detection System (IDS) help detect the Malware. Communication between at-least two parties using a network may uses Encryption-Decryption techniques to maintain privacy. And for authentication purpose apart from Encryption-Decryption techniques Hash Functions most widely used. The world is becoming more interconnected with the help of Internet and new networking technologies and there is huge amount of personal, military, commercial, and government information on networking infrastructures worldwide available (More specifically new way of payments in the forms of Cryptocurrency, BlockChain based methodology used here which is actually based on Hash). So it's important to find out who is transmitting critical data and who is receving, this will be take care by accountabilty policies managed by administrator. But how to identify wheather data received by one user is sent or e-mailed by valid user or the data received is actual one and not manipulated (i.e., Non-Repudation, Integrity). All these issues resolved by proving the authenticity of data and user with the help of hash function individually or with digital signatures scheme. As these systems quite helpful for us to manage various networking