2022 International Conference on Computers, Information Processing and Advanced Education (CIPAE) | 978-1-6654-6812-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/CIPAE55637.2022.00038

Analysis on Password Attack Model and Password Generation

Wenhan Jia
University of Cincinnati
Cincinnati, USA
wenhanja@mail.uc.edu

***Abstract*—Identity authentication is an important line of defense of network security, password has long been the mainstream way of identity authentication, password attack plays an important role in password security research. Probabilistic Context Free Grammar (PCFG) and the Markov chain-based model are the two most effective password attack methods. They can effectively model and describe the password from the substructure composition level and the character dependence level, respectively. This paper first analyzes the various encryption algorithms for cryptographic database, which are currently mainstream, and describes the comparison and strength of these algorithms. Moreover, this paper analyzes the current cipher structure within the password database. At last, this paper briefly describes the current method of password attacks and focuses on three most important methods, including Markov chain, OMEN algorithm and context-independent, to crack the password. This paper discusses the development of these three algorithms in current academic field, including the Recursive-OMEN algorithm based on structure partition and string reorganization, Adam algorithm based on dictionary attack, and genetic algorithm.**

Keywords—password attack, probabilistic context free grammar, OMEN algorithm, Markov chain, password structure, string reorganization, common character

I. Introduction

Identity authentication is a key line of defense for network security, and it is also the last line of defense to protect user's privacy [1]. Passwords are the main stream of identity authentication. Despite there are a great mass of issues in passwords regarding security and usability, and a large number of new authentication technologies have been proposed in succession. Password-based authentication method is still one of the most important authentication method due to its simplicity, low cost, and easiness in deployment [2]. Therefore, passwords have attracted widespread attention from scholars around the world in the recent decades, and a large number of significant researches have been published. It has been closely linked to personal information and property security as the rapid evolve of password authentication technology and frequently use in daily life. Therefore, password security research shows significant practical perspective in identity authentication.

II. Password Types

A key measure of the security of an encryption algorithm is the key strength, which gives the computational complexity by the power of 2. For example, a key strength of 128 gives a computational complexity of the and the attack algorithm needs to calculate to break.

A. Asymmetrical encryption algorithm aspects

At present, RSA algorithm is mainly used in China, which is gradually transitioning to SM2 national secret algorithm. The SM2 algorithm corresponds to the international ECC algorithm, and the digital signature, key exchange and public key encryption of SM2 correspond to the ECDSA, ECDH and ECIES of the ECC algorithm, respectively.

B. Hash algorithm aspects

At present, MD5 / SHA-1 algorithm is mainly adopted, and it is gradually transitioning to SM3 national secret algorithm. The SM3 algorithm corresponds to International SHA and is particularly similar to SHA-2. Table I describes the existing mainstream hash encryption algorithms as well as their comparison, including the number of input digits, output digits, number of iterations, packet length, and encryption intensity.

TABLE I. Comparison of the different hash encryption algorithms [5]

Algorithm	Input Bits	Output Bits	Iterations	Length	Strength
MD5	Unlimited	128	64	512	
SHA-1	264	160	80	512	60
SHA-224	264	224	64	512	112
SHA-256	264	256	64	1024	128
SHA-384	264	384	80	512	192
SHA-512	2128	512	80	1024	256
SM3	264	256	64	512	128

C. Symmetric encryption algorithm aspects

At present, DES / 3DES algorithm is mainly adopted, and is transition to SM4 national secret algorithm. The SM4 algorithm corresponds to the International AES algorithm, especially similar to the AES-128 algorithm. Table II describes the existing mainstream symmetric encryption algorithms, including the size, length, loops and strength.

978-1-6654-6812-1/22/$31.00 ©2022 IEEE
DOI 10.1109/CIPAE55637.2022.00038