SEMINARAS

Summary of Seminar on Password Security and Rainbow Tables

Mark Vainer

2025 m. rugsėjo 9 d. 09:00 val. S6(SRL-I) 401

Passwords are the most common and widely used method for user authentication. It allows users to gain access to systems and services using something (only) they know. Passwords are stored in an unreadable format, known as a hash value or digest, which is generated as an output from a cryptographic hash function which converts a password of an arbitrary length to a fixed-length value. This process adds a layer of security by making it more difficult for hackers to decipher the original password from the stored hash value. Cryptographic hash functions are designed as a one-way function, meaning that it is impossible to invert the function and find the original password given the hash value. Instead, malicious actors obtain the hash value via compromise or exfiltration and use indirect methods to find out what the password is. The most common and well-known approach is brute force attack, which is the most effective approach but also highly time consuming and resource-intensive, especially for long and complex passwords. Brute force attack involves trying every possible combination of characters until the correct password is found. Another approach is dictionary attack, which involves testing passwords from a pre-arranged list of words and known passwords from past data breaches. Dictionary attack is effective only in some cases, specifically for passwords that are simple, short, common, and easy to guess. If the passwords are long and complicated, they are unlikely to appear in any known dictionary.

Rainbow tables are a more efficient password cracking attack then brute-force attack and dictionary attack. It relies on the time-memory trade-off technique which occurs when an algorithm or program exchanges increased memory usage for reduced execution time.

For the rainbow table attack to work, a large table of passwords and hashes must be generated prior to the attack. Generation of such tables is very time consuming and requires a lot of computational power. In this seminar we will discuss the rainbow tables, their efficient generation and the implications of quantum computing in this field.

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev