

WHEN: Friday, May 5, 2006
WHERE: PGH 550
TIME: 1:30 PM

Host: Rakesh Verma

TITLE: Cracking passwords for fun and profit

SPEAKER: Vitaly Shmatikov, University of Texas at Austin

Abstract:

Human-memorable passwords are a mainstay of computer security. To decrease vulnerability of passwords to brute-force dictionary attacks, many organizations enforce complicated password-creation rules and require that passwords include numerals and special characters. We demonstrate that as long as passwords remain human-memorable, they are vulnerable to "smart-dictionary" attacks even when the space of potential passwords is large.

Our first insight is that the distribution of letters in easy-to-remember passwords is likely to be similar to the distribution of letters in the users' native language. Using standard Markov modeling techniques from natural language processing, this can be used to dramatically reduce the size of the password space to be searched. Our second contribution is an algorithm for efficient enumeration of the remaining password space. This allows application of time-space tradeoff techniques, limiting memory accesses to a relatively small table of "partial dictionary" sizes and enabling a very fast dictionary attack.

We evaluated our method on a database of real-world user password hashes. Our algorithm successfully recovered 67.6% of the passwords using a 2^{10^9} search space. This is a much higher percentage than Oechslin's "rainbow" attack, which is the fastest currently known technique for searching large keyspaces. These results call into question viability of human-memorable character-sequence passwords as an authentication mechanism.