

# Threats to Passwords

Passwords are used to protect our personal information on nearly all computers, but unless they are used properly the protection they provide may be very weak. This factsheet explains how passwords are attacked. The companion factsheet, 'Using Passwords' (PB/INFO/026), suggests ways to choose passwords to reduce the likelihood of attacks being successful.

Any server that uses passwords to authenticate users must itself store all the passwords. Normally these are stored in an encrypted form: when a user provides their password the same encryption is performed on it and the result compared with the stored version. If there is a match then the user is authenticated.

Most external attackers start by obtaining a copy of one or more encrypted passwords. Unfortunately, many network operating systems make this easy to do. Often all a remote computer needs to do is claim to be a client workstation and a server will hand over passwords. Alternatively an intruder may compromise or walk up to another computer on the same network and use it to steal passwords passing over the network. All systems should be configured and maintained securely to prevent remote compromises. The first stage in protecting passwords is therefore to configure networks and servers to protect the password information as well as they can. Servers should be set only to share authentication information with local clients, and firewalls used to block attempts to steal this information from outside the network. An intruder with physical access to a server or its backups can simply walk away with the password file. Once an intruder has obtained some encrypted passwords, by requesting them from a badly configured server or listening on the network, they can crack the password encryption on their own systems. They need not return to the target systems or networks until they know one or more valid username/password combinations.

The method used to crack passwords is very simple: generate all possible passwords according to some set of rules, encrypt them, and test them against the stolen version. The attacker can use any rule he can write down. For example, a password cracking program might try all the words in a dictionary (fewer than 100,000 attempts), words with some letters replaced by visually similar numbers, such as 'p455w0r6' (about 1 million), or even all possible combinations of the characters A to Z (about 200 billion).

These numbers seem huge, but modern desktop computers are amazingly fast. An efficient password cracking program can test several hundred thousand passwords per second. Generating and testing all possible alphabetic passwords of lengths up to 14 characters can take only a couple of hours. In the three-month lifetime used for many passwords, a single password cracking program can test about a trillion different guesses.

To give reasonable security against this kind of attack, a password must contain letters (both upper and lower case), digits and symbols, with no regular pattern that can be written into a rule. Using an eight character password, which is possible for humans to generate and remember, gives about a quadrillion different choices, an astronomical number but still giving the cracker about a 1/1000 chance of guessing each password before it is changed at the end of its lifetime.

Techniques have also been developed that split the cracking process into two stages: first generating a large set of tables (around the size of a modern PC hard disk) and then using these tables to crack individual passwords. Once an attacker has pre-computed the tables, or obtained them from another source, each individual password can be cracked much more quickly. To protect against an attacker who has generated the necessary tables, passwords should be ten or more characters in length if they are to be safe for three months.

Creating and remembering such complex passwords is a challenge for humans, but one that can be addressed by simple tricks. The factsheet 'Using Passwords' gives some ideas:

**<http://www.ja.net/services/publications/factsheets/026-using-passwords.pdf>**

JANET® is a registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of the trademark. JANET, the United Kingdom's education and research network, is funded by the Joint Information Systems Committee (JISC).