

## Getting back access to your password-protected laptop

### A story of sad (and eventually successful) experience of using a system logon password

Password protection is the simplest and most commonly used way for data protection from undesired intruders. In corporate environment users are usually forced to carefully select strong passwords following fixed and documented rules reflected in a corporate password policy.

In personal life users are free to choose if they need password protection for their personal data and very often people neglect such measures unless required, usually by Internet services. The prospect of choosing a sophisticated password, remembering it and entering it every time, when logging into the system, discourages most users, because all weigh their free time.

So, when it comes to a matter of private life data security, people are fully satisfied (or at least try to think so) just with restricting physical access to their desktops and laptops by leaving them locked in their apartments. But sometimes people can try to enhance their computer security and later regret it....

#### **Problem**

Alexandre Bykov from PR Newswire, the global leader in news and information distributor, begins his usual day by typing in his system password in order to access his computer - everyday routine: *"I use a password to log into Windows XP. I type it in, fetch myself a cup of coffee, and plunge into news and events."* Password-protected access is virtually mandatory in today's world.

As a bearer of an upwardly mobile profession, Alexandre prefers using laptops when out of office. *"I always use a laptop even at home. I find it practicable and very convenient. I'm not a gamer, nor video or music editor and so a laptop is quite enough for my regular email checks, presentations and Internet-surfing,"* shared Alexandre in a telephone interview. *"I am in charge of Russian companies and whirl in their news and willing or not tune in to all what's being currently broadcasted - IT security (especially laptop stealth) is in the forefront in news sphere. Finally, my sense of security has been stirred and I decided to set a more sophisticated logon password in my personal laptop...and got in an embarrassing situation of being locked out of my own computer, in consequence."* Alexandre simply forgot his password after a long holiday.

It has become so commonplace that users forget their passwords, having made them too complicated and become unable to remember them after a business trip or a vacation. *"I've been desperate at getting it back but no combination fitted. I thought I'd have to take my laptop to the nearest computer service, leave it there for who knows how long and hope my data will be safe. And I would do so, if I hadn't come across ElcomSoft, - they contacted me regarding their next press release on password recovery. I decided to take a chance."* After a short telephone conversation Alexandre got a feeling that the situation could be mended.

#### **Solution**

Luckily there were no EFS (Encrypting File System) working and therefore no threat to loose encrypted data (however that could be resolved as well\*). A simple booting from a special bootable CD-ROM allows full administrator privileges. *"I got an ISO-image from ElcomSoft and some instructions on how to use it,"* shared Alexandre, *"I merely copied it to the USB stick and started my laptop from it. In a couple of clicks I simply deleted that ill-fated password and could easily get back to my data."*

Truly, ESR works very simply. It first tries to restore passwords using a predefined attack (using both dictionary and direct search). In addition, some passwords can be extracted from cache, system services, autologon (if it is configured), and so on. Different combinations are tried (dictionary attack), for example, when the password is the same as the username with one or two digits appended at the end.

All this makes it fairly effective in restoring the lost password. This procedure does not take more than a few minutes. As a result, in many cases there is no need to reset the password, which ensures the security of all data on the machine. However, in the event the user doesn't use Encrypting File System, the forgotten password can easily be deleted without any unfortunate consequences.

Lost access to a locked computer scares users to death, as it seems there is no way out, at least without help from experts. ElcomSoft provides simple and convenient solution for quick access restoration.

---

*\* If a locked-out user prefers not to reset a lost password, but to recover it, one can use USB flash drive with ESR on it. With it, the user gets backup system files that contain password hashes and recovers plaintext passwords later on a different computer. So, a bootable USB flash drive can be very convenient in this case.*