Automatic system shutdown with PAM_TALLY2

Protect your mobile device against theft.

From Hans Freitag (Developer, CEO of Conesphere GmbH)

The screen Lock

- **Is unlocked frequently during the day.**
- **Should never allow any unauthorized access to the system.**

- **Users tent to have a short password here because they type it often.**

The Disk Passphrase

Especially on Systems that use suspend, the Disk Passphrase is not asked very often.

You can easily make your Disk Passphrase as long as needed for a good security without a high impact on useability.

The Attack Scenario

An attacker might try to keep your device running until he finds a way to break in.

I would do that, the OS has a much bigger attack surface than Disk Encryption.

Shutting the System down if Login Fails

Even Apple (IOS) does it!

There is lockdown and cryptfs_password available for Android.

There was no Linux/Unix solution.

Plugable Authentication Modules

Linux and other Unix Systems have a think called pam so you can dynamically add features to the user Authentication.

If you do it in PAM, every authentication process can benefit.

PAM Tally2

Is a PAM Module that is used to deny user login when auth Fails for a configurable amount of time.

All it needed was a patch to call a shutdown command when an account is blocked.

The Enhancement

https://github.com/zem/linux-pam/

auth required pam_tally2.so deny=4 even_deny_root cmd_onerr=/sbin/poweroff onerr=fail unlock_time=1200

Making Tallylog available to the User

https://github.com/zem/linux-pam/

auth required pam_tally2.so deny=4 user_access even_deny_root cmd_onerr=/sbin/poweroff onerr=fail unlock_time=1200

The user_access parameter wants a */var/log/tallylog dir where it stores a seperate logfile for each user. So non SUID Screenlockers will work.*