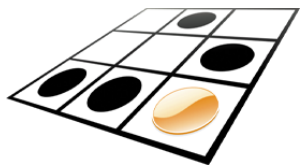
Некоторые механизмы безопасности ALT Mobile

Егор Шестаков, Андрей Савченко

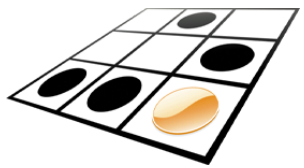
ООО «Базальт СПО»

XXI OSSDEVCONF
5 октября 2025



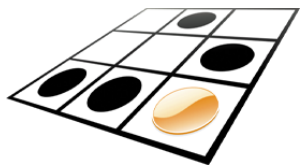
ALT Mobile

- ✔ Вся ОС на СПО
  - кроме некоторых прошивок периферийных устройств
- ✘ AOSP
- ✘ BSP Android
- ✔ Такой же дистрибутив Альт, как и остальные
- ✔ Пользователь управляет системой, а не система пользователем



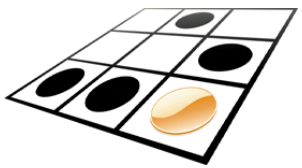
Полнодисковое шифрование LUKS

- Шифровать $HOME недостаточно:
  - конфиги, хеши паролей
  - логи, swap
- Новые вызовы:
  - Экранная клавиатура в initrd
  - Автоматизация установки с LUKS
- Secure Boot:
  - Возможно, но не нужно
  - Это инструмент vendor lock-in под соусом безопасности

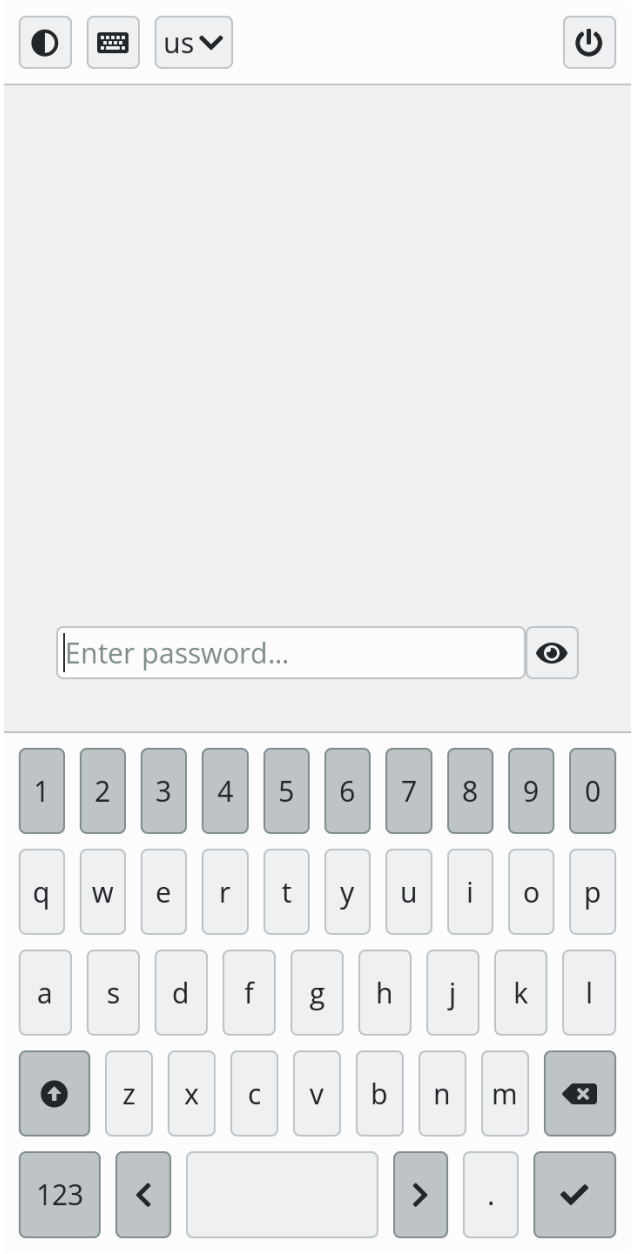


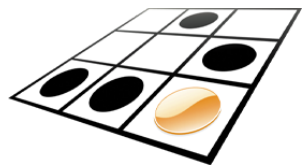
LUKS на мобильном

- unl0kr[1]:
  - рендеринг во фреймбуфер с помощью LVGL[2]
  - не зависит от аккселерации GPU
- make-initrd[3]:
  - угадайка для модулей touchscreen
  - поддержка unl0kr и f2fs fsck
- alt-rootfs-installer[4]:
  - поддержка LUKS и f2fs



Unl0kr


us
Enter password...
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
.



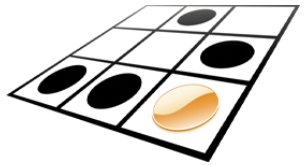
Тревожные пароли

Зачем:

- Безопасность
  - больше safety, чем security

Как:

- PAM FAlse BOttom[5]
  - пара {хеш, приложение}
  - произвольное количество действий
  - управление успешностью входа



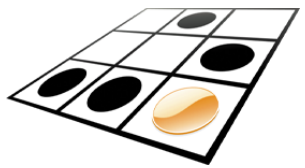
Пример использования

Задача

При вводе предопределённого *неправильного* пароля отправить sms на заданный номер

Шаг 1: получаем хеш пароля

```
$ mkpasswd -m gost-yescrypt
Пароль:
$gy$j9T$WHMM.EwOQHPp8oNpYVWDt.$az9B5u5Gj8d189VL3wKR4uUz6xzrApfMj57zJzGlA9D
```



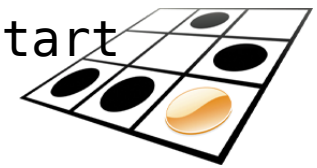
Пример использования

Шаг 2: конфигурация fabo

```
user altlinux
hash $gy$j9T$WHMM.EwOQHPp8oNpYVWDt.$az9B5u5Gj8d189VL3wKR4uUz6xzrApfMj57zJzGlA9D
command /usr/local/bin/send_emergency_sms
access deny
```

Шаг 3: включаем fabo

```
# cat /etc/pam.d/phosh
auth        optional    pam_fabo.so /etc/fabo_file
auth        include     system-auth
auth        optional    pam_gnome_keyring.so
session     include     system-auth
account     required    pam_permit.so
session     optional    pam_gnome_keyring.so auto_start
```

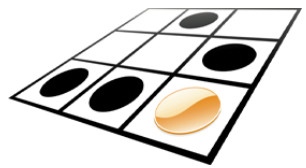


Пример использования

Шаг 4: задаём действие

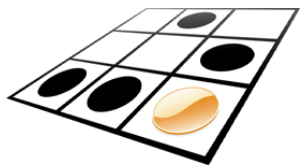
```
$ cat send_emergency_sms
#!/bin/sh -e
MSG_ID=‘mmcli -m any -K \
  –messaging-create-sms=”text=’Help!’,\
  number=’+71234567890’” \
  | grep -o ’/SMS/[[:digit:]]\+’\
  | grep -o ’[[:digit:]]\+’‘

mmcli -s $MSG_ID –send
```



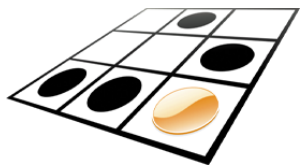
Ограничения

- Работа с правами пользователя:
  - для повышения привилегий нужны suid, capabilities, sudo...
- Нельзя просто так заменить $HOME:
  - пользовательская сессия его уже использует



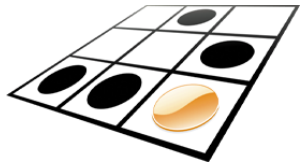
Дальнейшие идеи

- FABO:
  - ? поддержка TCB
- Разделение пина и пароля
  - сложный пароль для первичной авторизации
  - пин для быстрой вторичной (с лимитом)
- ГОСТ в LUKS
  - userspace crypto API



Итоги

- Разработанные решения универсальны
- Много доработок уже заапстримлено
- Проект открыт, документация есть на вики[6]:



Полезные ссылки I

- Unl0kr. — https://gitlab.com/postmarketOS/buffybox/-/tree/master/unl0kr.
- LVGL. — https://lvgl.io.
- Make-initrd. — https://github.com/osboot/make-initrd.
- ALT RootFS Installer. — https://git.altlinux.org/people/antohami/packages/alt-rootfs-installer.git.
- PAM FAlse BOttom. — https://git.altlinux.org/people/ved/public/pam_fabo.git.
- Alt Mobile Wiki. — https://www.altlinux.org/ALT_Mobile.