О возможностях применения в вузах аутентификации на основе персональных устройств

В.В. Буслюк, Д.А. Костюк, Д.И. Кульбеда, Н.А. Терешкевич, В.А. Юхно

Классификация

Средства аппаратной идентификации и/или аутентификации пользователей:

- аппаратные ключи защиты, взаимодействующие с компьютером
  - по шине USB
  - через устройство считывания контактной памяти (i-button)
  - по беспроводной передаче данных малого радиуса действия
- средства биометрии
  - сканеры отпечатков
  - какие-то другие системы распознавания (распознавание лица, рисунка радужной оболочки глаза и др.)

Аппаратная аутентификация студентов

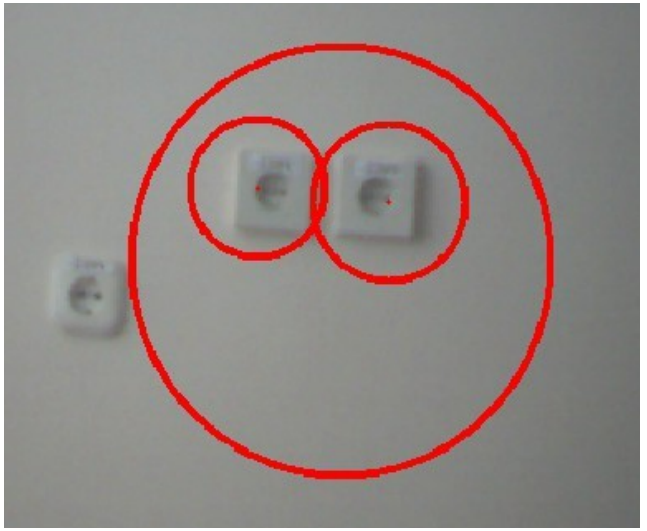
- Изначальная проблема аппаратных ключей – их нужно всё время закупать и выдавать пользователям
  - Бюджет на десятки тысяч студентов несоизмерим с идеей избавить их от необходимости вбивать пароль :)
  - Вам нужен какой-то более веский повод для закупок
- Однако неотделимой частью многих студентов являются персональные гаджеты, теоретически пригодные для однозначной идентификации

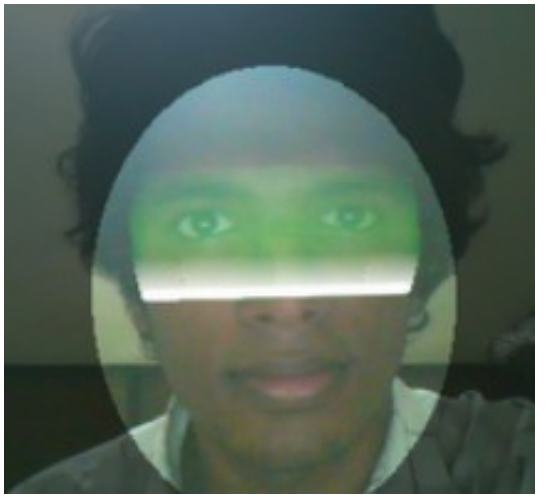
PAM-модули для биометрии в GNU/Linux

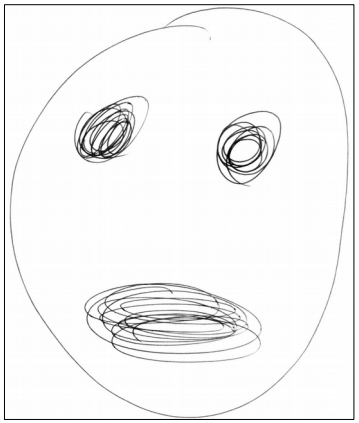
- **fprint** – проект, поддерживающий ряд стандартных сканеров отпечатков (как правило, встроенных в ноутбуки)
- **PAM Fingerprint** –для аутентификации с помощью датчика отпечатков в Arduino/Raspberry Pi
- **PAM_BFP** для USB-сканера Futronic
- **pam-bioapi** – фреймворк, являющийся ещё одной попыткой унифицировать считыватели отпечатков в Linux, сам по себе поддерживающий подгружаемые драйвера;
- **PAM face-recognition** – классический модуль, пытающийся распознать лицо пользователя с помощью веб-камеры и библиотеки OpenCV

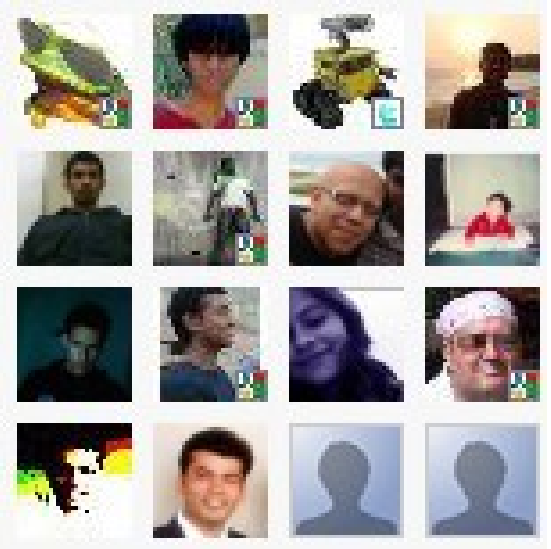
Пара слов о PAM face recognition

- Красиво, но несерьёзно :)









PAM-модули для аппаратной аутентификации

- **PAM-PKCS#11** – классический модуль для аутентификации (опционально, также идентификации) пользователей на основе смарт-карт
  - очень серьёзный, имеет полуэкспериментальную поддержку LDAP
- **pam_usb** – позволяет использовать USB-накопители в роли аппаратных ключей
  - известный и капризный
- **pam_nfc** – модуль для авторизации на основе ID-тегов карт RFID
  - Рекомендован в основном для идентификации и систем многофакторной аутентификации
- **pam-blue –** модуль для аутентификации с помощью гаджетов по протоколу bluetooth
  - в качестве ключа используется MAC-адрес Bluetooth-устройства
- **pamble** – аналог для Bluetooth Low Energy, написанный одним из соавторов
  - ориентирован на авторизацию с помощью популярных фитнес-трекеров Xiaomi

Пример подключения зоопарка

```
~/proj/pam_examples
❯ ./auth_test
login: jaffee
Failed to connect: Operation now in progress
* pam_usb v0.5.0
* Authentication request for user "jaffee" (auth_test)
* Device "16g" is not connected.
* Access denied.
Password:
Authenticated

~/proj/pam_examples
❯ ./auth_test
login: jaffee
Failed to connect: Operation now in progress
* pam_usb v0.5.0
* Authentication request for user "jaffee" (auth_test)
* Device "16g" is connected (good).
* Performing one time pad verification...
* Access granted.
Authenticated

~/proj/pam_examples
❯ ./auth_test
login: jaffee
Authenticated

~/proj/pam_examples
❯
```

```
1 #%PAM-1.0
2 auth  sufficient  pam_nfc.so
3 auth  sufficient  libpamble.so
4 auth  sufficient  pam_blue.so
5 auth  sufficient  pam_usb.so
6 auth  required  pam_unix.so nullok_secure
~
~
~
~
~
NORMAL  RO | auth_test                    unix | utf-8 | pamconf  16%  1:1
```

```
1 requisites = ( { username   = "jaffee";
2                  btaddr     = "C8:0F:10:3B:14:64"; }
3              );
4
5 // "C8:0F:10:3B:14:64"
~
~
~
NORMAL  RO | example.conf                 unix | utf-8 | no ft  20%  1:1
"/etc/security/example.conf" [readonly] 5L, 144C
```

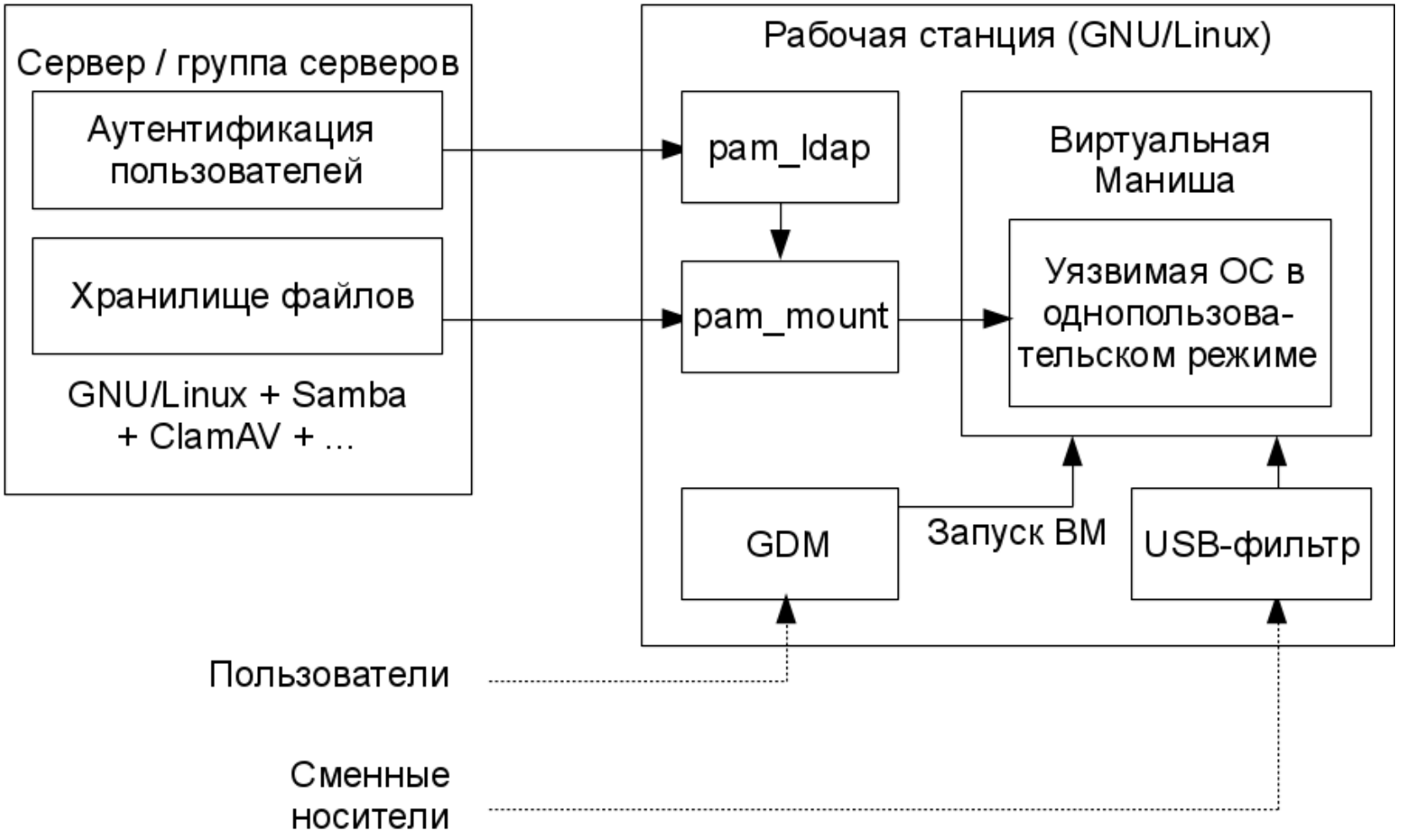
```
1 general {
2   timeout = 5;
3 }
4
5 jaffee = {
6   name = S950;
7   bluemac = E4:2D:02:96:42:CB;
8   timeout = 5;
9 }
NORMAL  RO | bluescan.conf                unix | utf-8 | no ft  11%  1:1
```

```
dev  › 1:ide  2:shell* 3:fish-                                  20:30 26 Jan
```

Задачи, не требующие криптостойкости...

- ...часто характерны для вузов
- аутентификация часто подменяет собой идентификацию пользователя
  - Доступ к личному расписанию
  - Выдача заданий
  - Результаты проверки работ
  - …
  - Доступ к компьютерам учебных классов?
- в случаях, когда надёжная аутентификация реально важна, её можно затребовать в процессе работы
  - Да хоть двухфакторную авторизацию ввести для доступа к нужному сервису

Почему компьютерам учебных классов в нашем случае нечего терять :)



Ещё немного белорусских реалий

- В белорусских вузах активно используются студенческие билеты с NFC
  - это разработка БГУ
    - ...и потому она активно используется :)
  - в основе – бесконтактные карты формата MIFARE Standard 4k
  - Билет хранит ФИО, номер, период действия, гражданство, вуз, факультет, специальность, группу и т. д.
  - Использовать их для чего-нибудь электронного очень заманчиво :)
    - возможно поэтому некоторые вузы поставили на входе турникет считывающий RFID-метки

Что можно прочесть без ключей?

** TagInfo scan (version 4.23) 2017-11-12 18:32:34 **
Report Type: External

-- IC INFO ------------------------------

IC manufacturer:
NXP Semiconductors

IC type:
MIFARE Classic (EV1) (MF1S70)

-- NDEF ------------------------------

No NDEF data storage present:
Maximum NDEF storage size after format: 3356 bytes

-- EXTRA ------------------------------

Memory size:
4 kB
* 32 sectors of 4 blocks and 8 sectors of 16 blocks
* 256 blocks, with 16 bytes per block

-- FULL SCAN ------------------------------

Technologies supported:
MIFARE Classic compatible
ISO/IEC 14443-3 (Type A) compatible
ISO/IEC 14443-2 (Type A) compatible

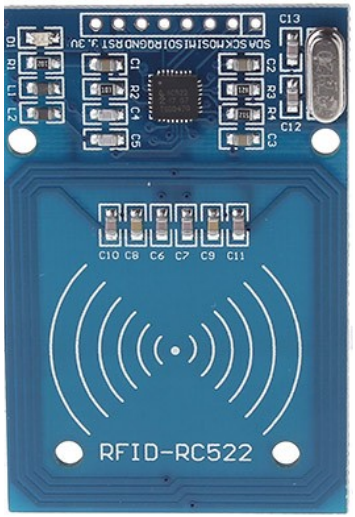
Detailed protocol information:
ID: 9C:D5:1A:25
ATQA: 0x0600
SAK: 0x18

Memory content:
Sector 0 (0x00)
[00] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[01] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[02] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[03] ??? XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
(unknown key) (unknown key)

Sector 1 (0x01)
[04] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[05] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[06] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[07] ??? XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
(unknown key) (unknown key)

Sector 2 (0x02)
[08] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[09] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0A] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0B] ??? XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
(unknown key) (unknown key)

Sector 3 (0x03)
[0C] ??? -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --



Проблемы аутентификации на основе личных гаджетов

- Радиус видимости гаджета
  - Логин пользователя вводится вручную
    - как страховка от ложных срабатываний
- Проблема с сетевыми учетными записями
  - Большинство немэйнстримных PAM-модулей не умеют работать с LDAP
  - Частичное решение - монтировать /home по сети (например, с autofs)
    - Не страшно при пониженных требованиях к безопасности
  - Частичное решение - «расползание» конфигов с идентификаторами в /etc рабочих станций (lsyncd, ...)
    - Защита строится не на сокрытии, а на сложности подделки