



Random generation

Internal random generator would be
a good idea, mixing dev/random,
Windows API, mouse & keyboard,
instead of just relying on underlying OS
for security.

possible alternative sources of entropy:

- ~~the~~ webcam
- microphone (in webcam)





QR Codes

masterkeys can be backed up and printed, when recovery is needed, bytes could be read more easily via QR codes than when typed into keyboard by hand.

RFID Tags

As suggested earlier, screen locking/unlocking should (or could) trigger also volume freezing/unfreezing. Locking can be triggered by external sources via plugins. One could source could be: RFID tags scanned at the computer terminal. It could both be used for locking and/or unlocking.





Regionalny
Ośrodek EFS

Sieradz



Regionalna
Izba Gospodarcza
Sieradz

www.sieradz.roEFS.pl

Startup speedup

Certain files are read at startup during boot sequence. These files could be read in advance, put in sequence, put in close locality, or otherwise preprocessed to decrease the bootup time.

Bluetooth/WiFi devices

Another mount/freeze/unfreeze/~~start~~
self destruct activation/deactivation external
signals:

detected presence of specific
bluetooth device by bluetooth adapter
(it must be in proximity to wake)

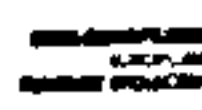
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
INICJATYWA WYKONAWCZA



Łódzkie
Województwo





Regionalny
Ośrodek EFS

Sieradz



Regionalna
Izba Gospodarcza
Sieradz

Performance measurement tool

FUSE ~~is~~ logging filesystem or
an extended Camdconice implementation
could be used for measuring patterns
of access. For example, Chronich/Frictor
can be measured for performance not only
~~through~~ through time elapsed ~~by~~ but can also
record what was read, when and how fast
down to discribe read() calls.

www.sieradz.roEFS.pl

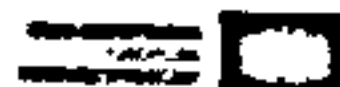
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
ROZWOJ CZŁOWIEKA



Łódzkie
Województwo



Regionalny Ośrodek EFS w Sieradzu
przy Regionalnej Izbie Gospodarczej
w Sieradzu

ul. Pułaskiego 5
60-200 Sieradz, tel 43 626 01 01,
fax 43 632 17 00

e-mail: info_sieradz@roEFS.pl
www.sieradz.roEFS.pl



memory wiping

* All critical ~~data~~ data should be wiped from RAM before deallocating. As for file content ~~set~~ and internal data structures, wiping can be added at later time under further investigation.

* Threat model should be ~~not~~ defined as attacker having privilege to run arbitrary programs ~~not~~

- (1) under guest account when mounted
- (2) under root account when unmounted

Specific attention should be diverted to

- Access control and unintentional exposure
- Memory leftovers being ~~leaked~~ left behind
- Disk block leftovers being leaked behind
- Means of subverting security ~~trying~~ during random searches
- Laboratory analysis of disk ~~usage~~ wear
- ~~Stop~~ recording MRU