www.sieradz.roEFS.pl

Random generation

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

possible alternative sources of entropy:

- ~~file~~ webcam
- microphone (in webcam)

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI

Łódzkie

UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

QR Codes

masterkeys can be backed up and printed, when recovery is needed, bytes could be read more easily via QR codes then 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.

www.sieradz.roEFS.pl

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI

Łódzkie nabiera prędkości

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 ~~kd~~ bootup time

Bluetooth / Wifi devices

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

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

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI

Łódzkie

Performance measument tool

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

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI

Łódzkie

memory wiping

- All critical data should be wiped from RAM before deallocating. As for file content and intend data structures, wiping can be added at later time under further milestone.
- Threat model should be defined as attacker having privilege to run arbitrary programs of
  (1) unprivileged guest account when mounted
  (2) unprivileged root account when unmounted

Specific attention should be diverted to
- Access control and unintentional exposure
- Memory leftovers being left behind
- Disk block leftovers being leaved behind
- Means of subverting security during random searches
- Laboratory analysis of disk after wear
- Desktop recording MRU

www.sieradz.roEFS.pl

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI

Łódzkie

Regionalny Ośrodek EFS w Sieradzu przy Regionalnej Izbie Gospodarczej w Sieradzu | ul. Pułaskiego 5 98-200 Sieradz, tel 43 858 91 91, fax 43 822 17 98 | e-mail: info.sieradz@roEFS.pl www.sieradz.roEFS.pl