DISCREETE LINUX

Goal

Discreete Linux is an operating system with the special purpose of protecting data (more precisely: people) against surveillance attacks with trojan software.

An Example of mass surveillance

With the QUANTUMTHEORY / FOXACID project, the Snowden documents showed a worldwide system of automated trojan infections. In the slides for the TURBINE project, the NSA states that it is designed to control Trojan infections "automated in millions of computers" - and that was the state of 2009. Today numerous commercial providers of surveillance tools like GAMMA are also selling Trojan software to dictatorships and states that proclaim torture.

BASIC CONSIDERATIONS

Discreete Linux provides an isolated, local working environment that is not accessible to spyware (Trojan software). Therefore, sensitive data can be processed, encrypted, and stored securely and is protected against such surveillance and espionage attacks.

Discreete Linux accomplishes this protection by the following the three general successive safety lines:

- Wall up the entrances
- Prevent spreading
- Wall up the exits

Discreet is based on two basic principles:

- Transparent development and free software
- User-friendly handling

I. WALL UP THE ENTRANCES

Close the entrance gates to the system so that malicious software can not invade it.

- PREVENT NETWORK ATTACKS
- ATTACKS VIA INTERNAL HARDDISKS
- MOUNT OPTIONS
- SHIELD USB AND FIREWIRE

II. PREVENT SPREADING

If an espionage software nevertheless succeeds in penetrating the system, further safety lines are intended to prevent it from causing lasting damage

- IMMUTABLE SYSTEM
- SIGNED KERNEL MODULES ONLY
- PREVENT THE ATTAINMENT OF ROOT PRIVILEGES

III. WALL UP THE EXITS

How to close and guard the exits.

USER-FRIENDLY HANDLING

Discreete Linux is less aimed at IT experts than whistleblowers, political and trade union activists, journalists, lawyers, human rights activists and other people who are threatened by targeted Trojan monitoring. It must therefore be easy to learn and to operate and, at the same time, it must prevent that inexperienced users Accidentally override the security through false behavior.

Live example how to work with Discreete Linux.

TRANSPARENT DEVELOPMENT AND FREE SOFTWARE

A system for security-critical applications such as Discreete Linux in our opinion should only be developed in an open, transparent process based on the principles of free software. All software, configurations and instructions for building the system are free software and released under the GPL. Discreete Linux is based on Debian.

How can you participate?