Зачем шифровать диск?

Если у вас паранойя по поводу слежки за вами, либо же у вас есть информация, которую хотелось бы скрыть от определенных лиц, то один из способов сокрытия содержимого носителя или его раздела – зашифровка всего содержимого определенными алгоритмами шифрования.

Существует множество ситуаций. Например, сломался компьютер, вы сдаёте его в сервисный центр на ремонт, при этом работник может легко вытащить информацию с любого носителя, после чего может проводить неограниченное кол-во атак. Либо же носитель могут украсть люди, которые заинтересованы в вашем взломе. Так же соответствующие органы власти имеют право конфисковать. Не говоря уже о банальной потери флэшки, внешнего жёсткого диска, либо диска.

В таких случаях следует позаботиться не только о том, чтобы нельзя было просто достать информацию с носителя, но и удостовериться в устойчивости к различным атакам, например, dictionary attack или brute-force, путём использования более надёжных алгоритмов шифрования, файлов-ключей, сложных паролей, больших кол-в итераций шифрования, скрытых томов и прочего.

В своей работе я рассматриваю возможность шифрования всей системы ОС Linux.