**Virtual Isolation**

**Separating Assets**

* Using different locations for different data by level of importance
* One for confidential, one for secret and one for top-secret
* Use different encryption keys for each
* NAS storage device with different volumes that can be individually encrypted

**Hidden Encrypted Volumes**

* Make the data harder to find for a hacker

**Use of separate session keys for messages (transporting data)**

**Portableapp.com, Pendriveapps.com**

* Standalone application that doesn’t require installation
* All data recorded by the app is stored in the one file location which isn’t the case with installed apps
* Installed apps have files based in different directories and make dir changes when data is recorded
  + This means that the file/app cant just be copy and pasted or moved in one click
* Using a portable app means all the data is in one file which makes movement and concealment of data easier
* The portable app (Firefox) can be downloaded on to a USB which is then used to run Firefox every time
  + All data Firefox records will be stored in that one file location on the USB including web history etc.
  + This means all data recorded by Firefox will be stored on the USB instead and can be moved or deleted in one-click
  + The USB can also be encrypted or stored in a hidden volume to provide more security of data
  + Could even use an encrypted USB and then store the portable app in an encrypted hidden volume on the USB with the keys stored elsewhere
    - This makes for well secured app data
  + They can also be stored in the cloud and run with a file syncing service and then run them remotely over the internet wherever you go
    - This means the application isn’t even stored locally, providing physical isolation as well – impossible for physical interception

**Plausible Deniability**

* Use a regular version of Firefox for normal browsing
* Use portable version for private browsing so that if you are forced to give up data, you can give up the normal version instead of your portable edition

**Authentic8**

**Cloudbrowser**

**Spikes Airgap**

**Spoons.net Browser Sandbox**

**Remote access**

* Remote use of a separate machine so malware can’t propagate to your machine
* XenServer, Cittrix, terminal services, remote desktop, XenDesktop

**Dual Boot**

Physical machines ship with a single OS

A dual boot allows for multiple OS for different security domains

* Can’t access multiple OS at the same time, like VMs

Can give a good privacy & security balance

* Due to being virtual, one OS could be used to compromise the other as there is no real (physical) isolation of the file systems in a dual boot
* May have different file system types, but not an actual security mechanism

Howtogeek.com has tutorials