**PEER-TO-PEER (P2P)**

Peer-to-peer file-sharing networks enable users to “publish” or “share” files – any file from music to video to spreadsheets. Current P2P clients allow users to share items in a particular folder and often direct users to move files to that folder. In normal operation, a P2P client simply writes files to disk as it downloads them and reads files from disk as it uploads them. There are several routes for confidential data to get on to the network: a user accidentally shares folders containing the information; a user stores music and other data in the same folder that is shared; a user downloads malware that, when executed, exposes files; or the client software has bugs that result in unintentional sharing of file directories [1].

Also, confidential files can be leaked through:

* **Email­ –** As Attachments.
* **Instant Messaging (IM)** – Files can be shared in many IM applications. E.g. Skype, MSN messenger etc. [3].
* **File Transfer Protocol (FTP)** - FTP is a popular protocol there is the likelihood it will be allowed through the firewall. FTP is probably more likely to be used in intentional leakage than unintentional leakage, due to the fact that uploading a file to an FTP server is generally not something an average user performs on a daily basis, nor would do inadvertently, as compared to attaching a file to an email [2] [3].

**REFERENCES**

1. <http://www.econinfosec.org/archive/weis2007/papers/43.pdf>
2. <https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931>
3. <https://www.sans.org/reading-room/whitepapers/analyst/data-leakage-landscape-data-leaks-generation-tools-apply-34695>