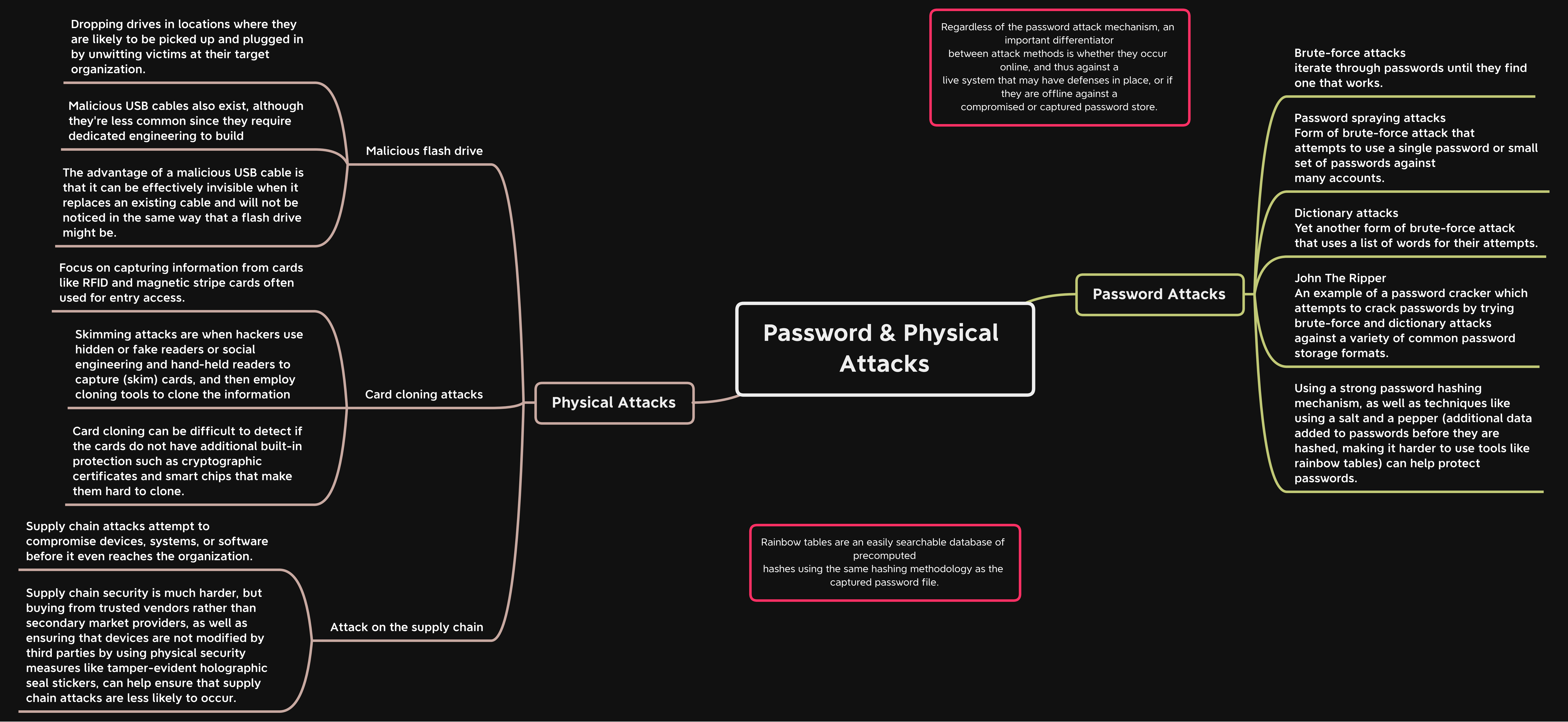

Password & Physical Attacks

Password Attacks

Brute-force attacks
iterate through passwords until they find one that works.

Password spraying attacks
Form of brute-force attack that attempts to use a single password or small set of passwords against many accounts.

Dictionary attacks
Yet another form of brute-force attack that uses a list of words for their attempts.

John The Ripper
An example of a password cracker which attempts to crack passwords by trying brute-force and dictionary attacks against a variety of common password storage formats.

Using a strong password hashing mechanism, as well as techniques like using a salt and a pepper (additional data added to passwords before they are hashed, making it harder to use tools like rainbow tables) can help protect passwords.

Regardless of the password attack mechanism, an important differentiator between attack methods is whether they occur online, and thus against a live system that may have defenses in place, or if they are offline against a compromised or captured password store.

Rainbow tables are an easily searchable database of precomputed hashes using the same hashing methodology as the captured password file.

Physical Attacks

Malicious flash drive

Dropping drives in locations where they are likely to be picked up and plugged in by unwitting victims at their target organization.

Malicious USB cables also exist, although they're less common since they require dedicated engineering to build

The advantage of a malicious USB cable is that it can be effectively invisible when it replaces an existing cable and will not be noticed in the same way that a flash drive might be.

Card cloning attacks

Focus on capturing information from cards like RFID and magnetic stripe cards often used for entry access.

Skimming attacks are when hackers use hidden or fake readers or social engineering and hand-held readers to capture (skim) cards, and then employ cloning tools to clone the information

Card cloning can be difficult to detect if the cards do not have additional built-in protection such as cryptographic certificates and smart chips that make them hard to clone.

Attack on the supply chain

Supply chain attacks attempt to compromise devices, systems, or software before it even reaches the organization.

Supply chain security is much harder, but buying from trusted vendors rather than secondary market providers, as well as ensuring that devices are not modified by third parties by using physical security measures like tamper-evident holographic seal stickers, can help ensure that supply chain attacks are less likely to occur.