Below is a **professionally formatted and sentence-by-sentence study note breakdown** of your document *“Multifactor Authentication Notes.docx”*. Every concept has been extracted, explained, and categorized for alignment with the **CompTIA A+ 220-1102 Exam**, specifically **Objective 2.1 – Security Concepts**. The structure is optimized for **clean pasting into Microsoft Word**, with proper numbering and minimal paragraph spacing.

**Multifactor Authentication – Study Notes - CompTIA A+ 220-1102 | Objective 2.1: Security Concepts**

**1. Identification vs. Authentication**

* **1.1 Identification:**
  + The user provides a **claim of identity**, such as a username, account number, or Social Security Number.
  + This step represents the **introduction** or declaration of the user’s identity.
* **1.2 Authentication:**
  + The system **verifies the user's identity** using a credential, such as a password, PIN, or token.
  + Occurs **after identification** is submitted.
  + Ensures that the claimed identity is valid and belongs to the person attempting access.

**2. Password Security Limitations**

* **2.1 Complexity Trends:**
  + Organizations try to increase password complexity with requirements such as:
    - Uppercase/lowercase letters
    - Numbers and symbols
    - Lengths exceeding 14 characters
* **2.2 Practical Risk:**
  + Users often:
    - Write down complex passwords
    - Reuse passwords across multiple systems
  + These behaviors **weaken actual security**.
* **2.3 Solution:**
  + Shift from complex passwords to **multifactor authentication (MFA)** for **stronger security**.

**3. What Is Multifactor Authentication (MFA)?**

* **Definition:**
  + MFA is the use of **two or more distinct authentication factors** to verify a user’s identity.
* **Factors of Authentication:**
  + **Knowledge** – something you know
  + **Ownership** – something you have
  + **Characteristic** – something you are
  + **Location** – somewhere you are
  + **Action** – something you do

**4. Authentication Factors Explained**

**4.1 Knowledge Factor (Something You Know):**

* Examples:
  + Passwords, PINs, security questions
  + Social Security Number, place of birth, mother’s maiden name

**4.2 Ownership Factor (Something You Have):**

* Examples:
  + **Token devices** (key fobs generating one-time codes)
  + **Smart cards** inserted into a reader
  + **USB encryption dongles**
  + **SMS codes** sent to smartphones
* These items serve as **physical proofs of identity**.

**4.3 Characteristic Factor (Something You Are):**

* Uses **biometric identifiers**, such as:
  + Fingerprints
  + Iris scans
  + Facial recognition
  + Voice recognition (used by some banks)
* **Device Examples:**
  + Older iPhones: fingerprint reader
  + Newer iPhones: dual camera facial unlock

**4.4 Location Factor (Somewhere You Are):**

* Determined via:
  + **IP address**
  + **GPS location** of the device
* Use Cases:
  + Unusual login locations may trigger alerts or request secondary verification
  + Some systems **restrict logins by region, state, or country**

**4.5 Action Factor (Something You Do):**

* Least commonly used in networks
* Examples:
  + How a person **signs a name**
  + Drawing a shape/pattern
  + **Walking behavior** in front of a sensor

**5. Single-Factor vs. Multi-Factor Authentication**

* **5.1 Single-Factor Authentication (SFA):**
  + Uses **only one type of factor**.
  + Example: Username + password = both knowledge factors → **still single-factor**.
* **5.2 Two-Factor Authentication (2FA):**
  + Requires **two different factor types**.
  + Example: Smart card (ownership) + PIN (knowledge)
  + If either factor is missing, access is denied.
* **5.3 Multifactor Authentication (MFA):**
  + Uses **two or more distinct factors** (can be 3, 4, or even 5).
  + Example:
    - Smart card (ownership)
    - PIN (knowledge)
    - Login location (location factor)

**6. One-Time Passwords (OTP)**

**6.1 Purpose and Benefit:**

* Improves security by using **passwords that expire quickly** and can't be reused.

**6.2 TOTP (Time-Based One-Time Password):**

* Generated using:
  + A **shared secret**
  + The **current time**
* Common in apps and physical tokens
* Password changes every **30–60 seconds**

**6.3 HOTP (HMAC-Based One-Time Password):**

* Uses:
  + **Shared secret**
  + A **counter synchronized** between client and server
* Generates a new OTP after each use

**7. In-Band vs. Out-of-Band Authentication**

**7.1 In-Band Authentication:**

* Both the login attempt and the second-factor verification occur on the **same device or channel**.
* Examples:
  + Logging into a website and receiving a one-time code to your **email on the same computer**
  + Logging into a mobile banking app and receiving a text message on the **same smartphone**
* **Less secure** due to **single point of compromise**

**7.2 Out-of-Band Authentication:**

* The second authentication factor is received via a **separate channel**.
* Example:
  + You log in on your laptop and enter a code shown on a **physical key fob.**
    - A **physical key fob** is a small, portable **hardware device** used in **multi-factor authentication (MFA)** to enhance security. It belongs to the category of "**something you have**" — also called the **ownership factor** in authentication models.
* **More secure** because the attacker must compromise **two systems or devices**

**8. Enterprise MFA Recommendation**

* For sensitive or enterprise environments, always prefer:
  + **Out-of-band 2FA or MFA**
  + **Combination of multiple distinct factors**
* MFA enhances defense against:
  + Credential theft
  + Social engineering
  + Phishing attempts