**Datensicherheit: Steganographie**

**1. Was ist Steganographie**

Definition:

Steganographie ist die Kunst und Wissenschaft, Informationen so zu verbergen, dass ihre Existenz geheim bleibt

Ziel:  
 Geheimhaltung von Informationen, indem sie in scheinbar harmlose Daten eingebettet werden, ohne dass ein Dritter bemerkt, dass ein Dritter bemerkt, dass eine Nachricht übermittelt wird

**2. Geschichte der Steganographie**

Antike:

Nachrichten wurden in Wachs- oder Tonkugeln versteckt, auf die Haut von Sklaven tätowiert oder in texten verborgen

Mittelalter:

Nutzung von Mikroschriften und unsichtbaren Tinten

Moderne:

Verstecken von Daten in digitalen Medien wie Bildern, Audio- und Videodateien

**3. Unterschiede Steganographie und Kryptographie**

Steganographie:

Verbirgt die Existenz einer Nachricht. Der Schwerpunkt liegt auf der Geheimhaltung der Kommunikation

Kryptographie:

Verschlüsselt den Inhalt einer Nachricht, ohne das Wissen über die Existenz der Nachricht zu beachten

Kombination:

Beide Techniken können kombiniert werden, um eine noch höhere Sicherheit zu erreichen

**4. Techniken der Steganographie**

Bild-Steganographie

LSB (Least Significant Bit)

Einbettung von Daten in den letzten Bit der Pixelwerte eines Bildes, um Veränderungen für das menschliche Auge unsichtbar zu machen

Audio-Steganographie

Echo-Verstecken

Verstecken von Daten in Audio-Echos, um die Veränderung des Originals unhörbar zu machen

Text-Steganographie

Whitespace-Methoden

Verstecken von Nachrichten in Leer- und Satzzeichen eines Textes

Video-Steganographie

Frame-Manipulation

Einbettung von Daten in bestimmten Frames eines Videos, ohne das visuelle Veränderungen bemerkbar sind

**5. Anwendung von Steganographie**

Militärische Kommunikation

Verstecken von Befehlen und geheimen Nachrichten in alltäglichen Daten, um Spionage zu verhindern

Digitales Wasserzeichen

Schutz vor Urheberrechten durch Einbetten von Identifikationsmerkmalen in Medien

Sicherheitsmaßnahmen

Verhindern der Entdeckung sensibler Informationen durch unbefugten Zugriff

**6. Herausforderungen und Risiken**

Erkennung durch Steganographie

Entwicklung von Techniken zur Entdeckung versteckter Informationen (statistische Analyse, ML)

Kapazitätsgrenze

Beschränkte Menge an Daten, die Verborgen werden können, ohne die Erkennbarkeit zu erhöhen

Missbrauch

Steganographie kann von Kriminellen genutzt werden, um illegale Aktivitäten zu verbergen

**7. Erkennung von Steganographie**

Visuelle und auditive Analyse

Sicht- oder hörbare Artefakte in Medien können auf versteckte Daten hinweisen

Statistische Analyse

Analyse von Mustern und Anomalien in digitalen Medien, die auf steganographische Inhalte hindeuten können

Softwaretools

z.B. Stegdetect (ist eig defunct seit 2019, aber Snowden hat seine Folien seit da nicht mehr aktualisiert)

**8. Fazit**

Steganographie bietet eine zusätzliche Sicherheitsebene durch die Geheimhaltung der Existent von Nachrichten. Trotz ihrer Vorteile muss sie mit Bedacht eingesetzt werden, da sie auch missbraucht werden kann.