|  |  |  |  |
| --- | --- | --- | --- |
| Une image contenant texte, Police, conception  Description générée automatiquement | Identification et authentification | |  |
| Thème du programme  Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et analyser | |
| Compétence | | Connaissance | |
| Identifier et appliquer les règles pour un usage raisonné des objets communicants et des environnements numériques (propriété intellectuelle, identité numérique, témoins de connexion, géolocalisation). | | Cybersécurité : protection des données personnelles, traces numériques (témoins de connexion, géolocalisation), identification, authentification, respect de la propriété intellectuelle ; | |

Aujourd’hui, de nombreux objets techniques sont connectés et échangent des informations.  
Il est donc essentiel de s’assurer que seuls les **émetteurs autorisés** puissent déclencher une action.  
Cette sécurité repose sur deux notions fondamentales : **l’identification** et **l’authentification**.

Les informations qui peuvent être ciblées par une attaque informatique :

* **Les identifiants d’un utilisateur** ou d’un appareil

*Exemple* : adresse MAC, identifiant de connexion, carte d’accès.

Permet de se faire passer pour quelqu’un d’autorisé (usurpation d’identité).



* **Les mots de passe** ou messages secrets

*Exemple* : message radio "GO", mot de passe de session, code PIN.

S’ils sont interceptés, l’attaquant peut déclencher une action sans autorisation.

* **Les données transmises** entre deux appareils

*Exemple* : température mesurée, coordonnées GPS, informations personnelles.

Ces données peuvent être espionnées ou modifiées.

* **Le programme ou le fonctionnement d’un appareil**

*Exemple* : un robot reçoit des ordres ou des mises à jour à distance.

Un pirate peut remplacer le programme pour changer le comportement de l’objet.

* **La fréquence ou le canal de communication**

*Exemple* : fréquence radio entre deux objets connectés.

S’il est découvert, l’attaquant peut écouter ou envoyer des messages malveillants.

* **Le comportement de l’utilisateur ou de l’appareil**

*Exemple* : horaires d’utilisation, trajets, habitudes.

Ces informations peuvent être utilisées à des fins de surveillance ou de manipulation.

Pour se protéger des dangers et garantir la sécurité des informations, il convient de **protéger l’accès aux appareils** (mot de passe, identifiant), **vérifier l’origine des messages** reçus (authentification), et **sécuriser les échanges de données** (fréquence, programme, contenu). Il est également essentiel de **limiter les informations transmises** et de **comprendre les risques liés aux objets connectés** pour mieux les anticiper.