LA TECHNOLOGIE AU COLLÈGE

Sciences et Techniques Industrielles

Portail national de ressources - éduscol

Région académique BOURGOGNE-FRANCHE-COMTÉ

CYCLE 4	Comment protéger d'une cyberattaque deux robots interagissant dans une zone de dépôt ?	NIVEAU QUATRIÈME

Présentation de la séquence :

La séquence, composée de trois séances, vise à développer les compétences liées à la cybersécurité (éventuellement déjà abordées en classe de 5eme).Les élèves vont ainsi revoir ou découvrir au travers d'une première séance les notions d'usurpation d'identité, d'identification ou d'authentification, de protection des données personnelles mais aussi des outils de cryptage des données (codage césar) et également des nouveaux métiers comme celui de Hacker éthique.
Dans la séance 2, après plusieurs manipulations, les élèves vont tester différentes méthodes de sécurisation d'une communication entre deux cartes électroniques et ainsi analyser leur pertinence.
Enfin, la séance 3 s'inscrit dans la continuité des deux séquences menées en 5eme, qui portaient sur le suivi de ligne par robot et l'assistance par caméra IA. Elle amène les élèves à comprendre comment protéger deux robots interagissant dans une zone de dépôt contre une tentative de piratage. À travers la découverte de l'authentification par numéro de série, ils apprennent à filtrer les messages et à sécuriser la communication entre objets connectés.

Thème abordé :	Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et à analyser
Attendu de fin de cycle :	Décrire les liens entre usages et évolutions technologiques des objets et des systèmes techniques

Compétences	**Connaissances**
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.
Identifier et appliquer les règles pour un usage raisonné des objets communicants et des environnements numériques (propriété intellectuelle, identité numérique, témoins de connexion, géolocalisation).	Cyberviolence : usurpation d'identité, usage détourné.

Thème abordé :	Structure, fonctionnement, comportement : des objets et des systèmes techniques à comprendre
Attendu de fin de cycle :	Comprendre et modifier un programme associé à une fonctionnalité d'un objet ou d'un système technique

Compétences	**Connaissances**
Analyser les données et en déduire des modifications à apporter au programme	-déclenchement d'une séquence d'instructions par un évènement ;
Compléter un programme pour répondre à une fonctionnalité d'un OST.	-instruction conditionnelle ;

PROPOSITION DE DÉROULEMENT DE LA SÉQUENCE

Séance 1 : (80 mn) Protection des données.

Situation déclenchante : (5mn) Discussion commune animée par le professeur sur " Ce qu'est la cybersécurité " pour les élèves et " la protection des données ". Lecture commune du paragraphe d'introduction de la séance 1.

Problématique : Quels moyens avons-nous pour sécuriser nos données, se protéger des arnaques. Comment font les entreprises pour se protéger ?

Investigations :

Travail 1 : Vidéos données par le professeur à visionner **(20 mn)**
Le professeur propose 4 petites vidéos sur la facilité à " craquer " un mot de passe ce qui amène les élèves à prendre conscience de l'importance de la configuration de leur mot de passe (nombres de caractères, ratio chiffres – lettres – caractères spéciaux, majuscules, minuscules, etc…)
Les élèves répondent au questionnaire sur les vidéos, puis ils ouvrent le site internet (https://ssi.economie.gouv.fr/motdepasse) pour tester une série de mot de passe.
Les élèves rédigent leur propre conclusion sur ce qu'est un bon mot de passe.

Travail 2 : technique du " hameçonnage " ou " phishing " **(15 mn)**
Ouverture du site internet https://phishingquiz.withgoogle.com/?hl=fr pour découvrir et sensibiliser les élèves à cette forme d'escroquerie.
Les élèves répondent à une petite série de questions et rédigent leur propre conclusion.

Travail 3 : Le cryptage des données…. **(20 mn)**
Le professeur propose aux élèves une vidéo sur le " chiffrement des données ".
Les élèves répondent à 2 questions qui introduisent la méthode César (méthode de cryptage). En exercice, ils réalisent ensuite le cryptage d'un message (code d'entrée du portail du collège) qu'un professeur envoie à un de ses collègues.

Travail 4 : Ce que font les entreprises pour se protéger des cyber-attaques (**15 mn)**
Les élèves visionnent les deux vidéos proposées par le professeur qui introduisent et présentent le métier d'hacker éthique et complètent les questions de leur activité.

Bilan de séance : (5 mn)
La cybersécurité est devenue l'affaire de tous. En effet les piratages informatiques et attaques sont de plus en plus présents de nos jours. Il est donc prépondérant de protéger ses données (soit par mots de passe ou cryptage) et d'analyser chaque mail ou sms reçus de manière à ne pas tomber dans les pièges tendus par des personnes malveillantes. Le métier d'hacker éthique est d'ailleurs apparu pour permettre aux entreprises de tester leur système de sécurité en analysant les failles possibles de leur système.

Ressources pour le professeur	Ressources pour les élèves
Vidéos mot de passe : 1 - https://www.youtube.com/shorts/kSg9YLP_2_E 2 - https://www.youtube.com/shorts/SziCWSTS5BM 3 - https://www.youtube.com/watch?v=YI-6nZFxwNg 4 - https://www.youtube.com/shorts/omHN1gwkVkM Site internet : http://ssi.economie.gouv.fr/motdepasse Hameçonnage : https://phishingquiz.withgoogle.com/?hl=fr Chiffrement des données : https://www.google.com/search?client=firefox-b-&channel=entpr&q=video+le+chiffrement+des+donn%C3	Vidéos proposées dans la séance Fiche élèves séance 1 Fiche ressource "Méthode de cryptage césar" Site internet : http://ssi.economie.gouv.fr/motdepasse Hameçonnage : https://phishingquiz.withgoogle.com/?hl=fr Chiffrement des données : https://www.google.com/search?client=firefox-b-&channel=entpr&q=video+le+chiffrement+des+donn%C3%A9es#fpstate=ive&vld=cid:6c295b33,vid:xFt_luN7Fyo,st:0

%A9es#fpstate=ive&vld=cid:6c295b33,vid:xFt_luN7Fyo,st:0 Hacker éthique : 1 - https://www.youtube.com/watch?v=iVrmzwbl8oo 2 - https://www.youtube.com/watch?v=s8Rs0cfDT90 Fiche professeur séance 1 corrigée Fiche ressource "Méthode de cryptage César" Structuration de connaissances cyber-sécurité	Hacker éthique : 1 - https://www.youtube.com/watch?v=iVrmzwbl8oo 2 - https://www.youtube.com/watch?v=s8Rs0cfDT90 Vidéo "le chiffrement des données" https://www.google.com/search?client=firefox-b-&channel=entpr&q=video+le+chiffrement+des+donn%C3%A9es#fpstate=ive&vld=cid:6c295b33,vid:xFt_luN7Fyo,st:0 Structuration de connaissances cyber-sécurité

Séance 2 – 80 min - 1H20

Situation déclenchante : (10mn) : le professeur montre la vidéo (Fonctionnement manuel des robots) de deux robots pilotés par l'homme : appui sur le bouton A pour lancer le robot 1 puis quand il a terminé son cycle, appui sur l'autre bouton A pour lancer le robot 2.

Problématique : comment permettre à deux robots d'interagir ensemble sans intervention humaine ? Le système est-il protégé contre toutes formes d'intrusion ?

Investigations

Partie 1 : (30 mn) Vidéo (Fonctionnement automatique des robots) **des deux robots fonctionnant en autonomie :** rendre autonome les deux robots et leur permettre d'interagir ensemble.
- les élèves ont à leur disposition les vidéos données par le professeur et le programme qui pilote les deux robots " Fonctionnement-manuel-robot 1 et 2"
- les élèves analysent les différentes parties de ce programme en complétant le travail 1 de leur fiche d'activité.
- à l'aide de la fiche ressource " Comment faire communiquer 2 cartes" et un exercice d'application sur une prise de température ambiante, les élèves modifient ensuite ce programme pour rendre les robots autonomes :

1 – suppression du bloc " lorsque bouton A pressé" pour la carte B.
2 – Création du bloc fréquence radio (fiche ressources sur la programmation logiciel makecode).
3 – Création du bloc "envoi et réception de messages" (mot de passe GO) pour formaliser la communication (bloc "receivedstring" à introduire sur la carte B).
4 – Appui sur le bouton A de la carte 1 pour lancer le cycle complet.

Test du bon fonctionnement par les élèves.

Partie 2 : (25 mn) Introduction d'un hacker dans le programme des robots.
- Les élèves ouvrent un programme donné par le professeur " Recherche-fréquence-Hacker ", et réalisent un exercice de recherche de fréquence.
- Les élèves trouvent avec ce programme la fréquence radio émise pour la communication entre les deux robots. Ils peuvent ainsi "interférer" dans cette communication car ils peuvent capter le message Go qui est l'ordre donné par le robot 1 au robot 2 pour que celui-ci commence son cycle.

Travail 3 : test de piratage (**10 mn)**
- les élèves testent le programme "Fonctionnement-autonome-robot 1 et 2" et interfèrent dans celui-ci via la carte Hacker : ils envoient des ordres (message GO toutes les 50 ms) dans le système.
- les élèves testent le dysfonctionnement du système.

Bilan de séance : (5 mn)
Il apparait très facile pour un hacker de trouver la fréquence de communication radio entre deux robots. Cela montre que seul un mot de passe et une radio fréquence ne suffisent pas à protéger notre système et notre programme.
Il est primordial de sécuriser davantage notre système et notre programme en trouvant des solutions bien plus sécurisées et difficiles à contourner.

Ressources pour le professeur	Ressources pour les élèves
Fiche professeur séance 2 corrigée Fiche ressource " Faire communiquer 2 cartes microbit" Fiche ressource " Recherche fréquence" Site internet : https://makecode.microbit.org/ **Programmes :** " Fonctionnement-manuel-robot 1" et Fonctionnement-manuel-robot 2". "Fonctionnement-autonome-Robot-A" "Fonctionnement-autonome-Robot-B" " Recherche-fréquence-Hacker". " Ecoute-hacker". " Carte-A-test température" " Carte-B-test température" " Carte-A-et-B-test-température-blocs-séparés". Vidéo "fonctionnement automatique robots" Vidéo "fonctionnement manuel des robots " Structuration de connaissances instruction conditionnelle	Fiche élève séance 2 Programme test : - " Fonctionnement-manuel-robot 1" - " Fonctionnement-manuel-robot 2". - " Carte-A-et-B-test-température-blocs-séparés ". - " Recherche-fréquence-Hacker". - " Carte-A-et-B-test-température-blocs-séparés". Fiche ressource "Recherche fréquence". Fiche ressource "Faire communiquer 2 cartes". Site internet : https://makecode.microbit.org/ Vidéo "fonctionnement automatique robots" Vidéo "fonctionnement manuel des robots " Structuration de connaissances instruction conditionnelle

Séance 3 – 80 min – 1H20
Description de la séance 3.

Situation déclenchante (10 min)
Le professeur propose une vidéo (fonctionnement automatique robots) montrant le fonctionnement des deux robots avec les programmes conçus en séance 2.
Dans cette séquence, le robot 1 démarre après un appui sur le bouton A, puis envoie un message GO via la fréquence radio pour déclencher automatiquement le départ du robot 2.

Une personne manipule ensuite une troisième carte micro-bit (carte pirate) et envoie également le message GO. Le robot B réagit de la même manière, bien que l'ordre ne provienne pas de la carte A. il y a collision entre les robots.
Cette démonstration permet de mettre en évidence la vulnérabilité du système.

Le professeur introduit alors la notion d'authentification : il explique qu'un message ne devrait être pris en compte que s'il provient d'un émetteur autorisé, identifiable par son numéro de série unique.

Problématique
Comment éviter le piratage de la commande du robot par n'importe quelle autre carte ?

Investigations
Partie 1 : découverte d'un système non sécurisé (20 min)

Les élèves testent un programme simple dans lequel la carte A envoie un message "ACCES", et la carte B réagit automatiquement. En changeant de carte A, ils constatent que la carte B accepte tous les messages, sans distinction. Cela les amène à conclure que le système n'est pas sécurisé : il réagit à n'importe quel message "ACCES" sans tenir compte de l'émetteur. Les élèves complètent le travail 1 de leur fiche d'activité à partir de cette observation.

Partie 2 : identification de l'émetteur et filtrage (20 min)

Le professeur engage ensuite un questionnement pour faire émerger la nécessité d'identifier l'expéditeur du message. Les élèves sont amenés à découvrir que chaque carte micro-bit possède un numéro de série unique. À l'aide du bloc " **numéro de série du périphérique** ", ils relèvent celui de leur carte. En activant " **radio régler le numéro de série de transmission vrai** ", la carte A envoie automatiquement ce numéro avec chaque message. Ils intègrent alors ce filtrage dans le programme de la carte B pour que celle-ci n'accepte les messages que si l'émetteur est bien autorisé. Les élèves valident ce fonctionnement par des tests avec plusieurs cartes.

Partie 3 : sécurisation de la communication entre les robots (20 min)

Les élèves réutilisent les programmes des robots conçus en séance 2. La carte A envoie toujours le message "GO", mais cette fois avec son numéro de série. La carte B est modifiée pour n'accepter ce message que si le numéro correspond à celui de la carte autorisée. Après modification, les élèves testent leur système : si la carte A envoie le message, le robot 2 réagit normalement. Si une autre carte envoie ce même message, le robot 2 ne réagit pas. Les élèves complètent le travail 2 de leur fiche d'activité, validant ainsi la sécurisation du système.

Bilan de séance (5 min)
En conclusion, les élèves comprennent qu'un simple mot-clé et une fréquence radio ne suffisent pas à sécuriser un système. La vérification de l'identité de l'émetteur permet d'empêcher toute tentative d'intrusion. Grâce à l'ajout d'un filtre basé sur le numéro de série, la communication entre les deux robots devient plus fiable et protégée contre les attaques. Le professeur souligne l'importance de l'authentification dans tout échange entre objets connectés.

Synthèse (5 min)
De nombreux objets techniques échangent aujourd'hui des données, ce qui les rend vulnérables aux intrusions. Les attaques peuvent cibler des identifiants, des messages, des programmes ou des habitudes d'utilisation. Pour se protéger, il est essentiel de vérifier l'identité de l'émetteur, de sécuriser les échanges et de limiter les données partagées. L'identification et l'authentification sont donc des clés de la cybersécurité.

Ressources pour le professeur	**Ressources pour les élèves**
Fiche professeur séance 3 corrigée Site internet : https://makecode.microbit.org/ **Programmes :** "Fonctionnement-autonome-Robot-1" "Fonctionnement-autonome-Robot-2" "Programme-carte-A-séance-3-partie-1" "Programme-carte-B-séance-3-partie-1" Vidéo "attaque pirate" Structuration de connaissances identification-authentification	Fiche élève séance 3 Site internet : https://makecode.microbit.org/ **Programmes :** "Fonctionnement-autonome-Robot-1" "Fonctionnement-autonome-Robot-2" "Programme-carte-A-séance-3-partie-1" "Programme-carte-B-séance-3-partie-1" Vidéo "attaque pirate" Structuration de connaissances identification-authentification