Micro:Bit Activities Leveling w/ SWBAT

Microbit101 - Monday PM Part 1 2

Name Game - Monday PM Part 2 2

Beacons - Tuesday 3

Microbot - Wednesday 4

Password Cracking & Encoding/Encryption - Thursday 5

Garage Door - Extension 6

MicroPay - Extension 6

CEDAR

CYBERSECURITY EDUCATION AND RESEARCH CENTER
@ The University of Wyoming
www.uwyo.edu/CEDAR
www.cowpokes.camp
www.uwcedar.io/community/cowpokes/wikis

Microbit101 - Monday PM Part 1

Cybersecurity Principle(s): Keep it Simple
Introductory programming concepts will be taught to bring students to a baseline understanding of programming that will enable them to complete the activities throughout the week. Students will be taught and understand that the following simple constructs can be used in powerful ways.

Novice: SWBAT:

- ❏ declare, use, and change the value of variables.
- ❏ list and identify the main types a variable can hold: numbers, strings, and booleans.

Intermediate: SWBAT

- ❏ identify instances in a program where repetitive code can be replaced with a loop
- ❏ create a program that utilizes a conditional statement to follow different logical paths.

Expert: SWBAT

- ❏ create functional and useful programs through the use of:
    - ❏ variables,
    - ❏ conditional statements, and
    - ❏ loops

Extension:

- ❏ Students will **investigate** then **use** the radio functionality of the Micro:bit to send and receive radio signals.

Name Game - Monday PM Part 2

Cybersecurity Principle(s): Keep It Simple
Students will put their newly developed programming skills to use in a friendly competition where they race to send their team name over a random radio channel to the instructor.

Novice: SWBAT:

- ❏ repeat instructions to use the micro:bits to send out a message on radio channels

Intermediate: SWBAT

- ❏ Implement variables and conditional statements to send out a message on radio channels with the ability to switch through channels more quickly.

Expert: SWBAT

- ❏ Design a loop to send radio messages faster than a human would be able to

Beacons - Tuesday

Cybersecurity Principle(s): Confidentiality/Integrity/Availability
The objective of the beacons lab is to introduce them to cybersecurity principles- confidentiality, integrity and availability. Students will be taught to send and receive messages over radio communication on micro:bit and make the communication more secure with each step.

Novice: SWBAT:

- ❑ receive a secret message on radio channels and display it on their micro:bits.

Intermediate: SWBAT

- ❑ Create a manual tuner that tunes to different channels to receive a secret message on radio channels
- ❑ Implement a mechanism to store messages on the micro:bits and display them later.

Expert: SWBAT

- ❑ Develop a loop that:
    - ❑ automatically searches through all the channels and
    - ❑ receives a secret message on radio channels,
    - ❑ store them and display them on their micro:bits.

Extension: Students implement a loop that searches the first 10 channels on the micro:bit and displays the channel with the highest number of beacons.

Microbot - Wednesday

Cybersecurity Principle(s): Defense in Dept
Students will be introduced to attacks like Denial of Service (DoS) and replay attacks. They will learn to control a robot and use it for navigation. They will also learn how to make their robots secure from on-going replay attacks and hacking.

Novice: SWBAT

- ❏ Use radio commands to control a robot
- ❏ Use the robot for simple navigation (left, right and forward).

Intermediate: SWBAT

- ❏ develop a program that ensures secure communication between the micro:bits by sending and receiving messages on a secret channel.

Expert: SWBAT

- ❏ Design a robots secured against hacking by sending out encrypted messages for commands (left, right and forward).

Extension: Students will be able to create a communication strategy to defend their robots from replay attacks.

Password Cracking & Encoding/Encryption - Thursday

Cybersecurity Principle(s): Confidentiality/Integrity/Availability and Thinking like an adversary
This activity introduces students to basic cryptography and the dangers (and benefits) of using websites with insecure encryption or using a password based off of personal information.

Novice: SWBAT decode a secret message encoded using a Caesar cipher as well as use background information about an individual to guess a simple password.

Intermediate: Students will be able to decode a secret message encoded using a keypad cipher as well as use background information about an individual to guess an intermediate strength password.

Expert: Students will be able to decode a secret message encoded using a Pigpen cipher as well as use background information about an individual to guess a complex password.

Garage Door - Extension

Cybersecurity Principle(s): Confidentiality/Integrity & KIS
The objective of this activity is to teach students to think like an adversary by teaching them to code program that intercepts the communication of a garage door transmitter and receiver.

Novice: Students will be able to program a garage door lock /unlock feature using a single channel radio communication over garage door transmitter and garage door receiver. Students will also be able to intercept these communications as they happen on a single channel.

Intermediate: Students will be able to program a communication between the garage door transmitter and garage door receiver on different channels. Students will be able to intercept the communications between the transmitter and receiver pair on different channels.

Expert: Students will be able to build an attacker program that intercepts the communication between a garage door transmitter and receiver by going through a wide range of possible codes communicated between the transmitter and the receiver.

MicroPay - Extension

Cybersecurity Principle(s): CIA
This activity reinforces the concepts of data integrity and confidentiality by showing weaknesses (and developing fixes) in a simulated peer-to-peer payment system.

Novice: Students will be able to recognize a simulated integrity weakness in the p2p payment system and develop and program a solution to fix the weakness.

Intermediate: Students will be able to identify a confidentiality weakness in the simulated p2p payments system and develop and program a solution to fix the weakness.

Expert: Students will be able to program a username and password check to validate confidentiality in the p2p system.

Extension: Students should be able to program a handshake protocol to transfer coins to another micro:bit.