

Introductie

In dit project leer je de basissetup zender, ontvanger, hacker kennen waarop we in onze andere projecten van het cybersecurity traject gaan verder bouwen. Informatie in de vorm van *cleartext* wordt via de bluetoothsignalen van een micro:bit tussen TI-Nspires verstuurd, door de zender naar de ontvanger. Een hacker kan vervolgens op een eenvoudige manier deze informatie onderscheppen.

Achtergrondinformatie

- **Radiogolven** zijn elektromagnetische straling, zoals licht, maar met een lagere frequentie. Alle elektromagnetische straling verplaatst zich met de snelheid van het licht, $3,0 \times 10^8$ m/s. Radiogolven kunnen korte of lange afstanden afleggen, afhankelijk van het elektrische vermogen van de radiozender. De radiogolven van de micro:bit kunnen ongeveer 70 meter afleggen in vacuüm. Kijk eens op de achterkant van je micro:bit, in de linker bovenhoek. Kun je de gouden antenne van de radiogolven terugvinden? Dit is waar de radiogolven in en uit de kaart gaan.
- De micro:bit zendt radiogolven uit en ontvangt ze, met frequenties die variëren van 2402 - 2486 megahertz; dit bereik wordt het spectrum van de radiogolven genoemd. Het spectrum van de micro:bit is verdeeld in 1 MHz brede banden, die **kanalen** worden genoemd. Er zijn **84** verschillende radiokanalen, variërend van 0 tot 83, op de micro:bit. Twee of meer micro:bits moeten hetzelfde kanaal delen om met elkaar te kunnen communiceren. (Denk aan walkietalkies die ook op dezelfde frequentie moeten zitten)
- **Tekstberichten** worden aan radiogolven toegevoegd doormiddel van de python modules die je op de laatste pagina van de code kan terugvinden. De tekstberichten worden in een **functie** geplaatst, inclusief aanvullende informatie die nodig is voor verzenden, ontvangen en foutcontrole.
- Naast de micro:bit zijn radiokanalen, is er ook een **softwaregroep**. Het groepsnummer maakt deel uit van het berichtpakket dat wordt gebruikt om de gegevens te verzenden en ontvangen, vergelijkbaar met TCP/IP-pakketten die op het internet worden gebruikt. De groep is één byte van het pakket en varieert van 0 tot 255.
- Om twee radio's te laten communiceren, moeten ze **hetzelfde kanaal en dezelfde groep** delen.
- Wanneer een tekstbericht in leesbare tekens over de radio wordt verzonden, wordt dit **cleartext** genoemd. Dit is kwetsbaar voor afluisteren door een onbekende hacker die op hetzelfde radiokanaal en dezelfde groep luistert. Dit type hacking wordt een "**man-in-the-middle aanval**" genoemd en wordt vaak gebruikt om informatie die doorgestuurd wordt over het internet te onderscheppen.

Wat is jouw opdracht?

1. Organiseer je team:
 - a. Werk in een team met ten minste twee anderen, ieder met een Nspire CX II-rekenmachine en een micro:bit.
 - b. Je docent wijst je team een radiokanaalnummer toe. Verander het groepsnummer niet.
 - c. Elk groepslid kiest een rol: zender, ontvanger of hacker.
2. Verstuur een tekstbericht:
 - De **ontvanger**
 - Zal doorgaan naar het tabblad '**student_ontvanger.py**', het kanaal wijzigen naar het toegewezen kanaalnummer en het programma uitvoeren (ctrl+r) voordat de zender het programma uitvoert.

- De zender
 - Zal doorgaan naar het tabblad 'student_zender.py', de berichtstring bewerken, het kanaal wijzigen naar het toegewezen kanaalnummer, en het programma uitvoeren (ctrl+r) nadat de ontvanger en hacker hun programma hebben gestart.
- De hacker
 - Zal doorgaan naar 'student_hacker.py', het kanaal wijzigen naar het toegewezen kanaalnummer, en het programma uitvoeren (ctrl+r) voordat de zender het programma start.
- Nadat je team de activiteit heeft uitgevoerd, kan de zender het programma wijzigen naar een ander kanaalnummer (0-83) en ook het bericht aanpassen. De zender fluistert het nieuwe kanaalnummer naar de ontvanger, die dan het programma naar hetzelfde kanaalnummer moet aanpassen. Vertel de hacker niets; **houd het privé!** Voer de activiteit daarna opnieuw uit. Krijgt de hacker het nieuwe bericht? Kun je uitleggen waarom?

De code

Zender

```

student_zender.py 11/11
from microbit_radio import *
# Het geheime kanaal en de groep moeten
# hetzelfde zijn als dat van de ontvanger.

kanaal = 1
groep = 1
bericht = "Goud verstopt in koekjestrommel."
clear_history()
print("\nBericht =",bericht)
tx(bericht,kanaal,groep)
    
```

Ontvanger

```

*student Ontvanger.py 11/11
from microbit_radio import *
# Het geheime kanaal en de groep moeten
# hetzelfde zijn als dat van de zender.

kanaal = 1
groep = 1
clear_history()
bericht = rx(kanaal,groep)
print("\nBericht =",bericht)
    
```

Hacker

```

student_hacker.py 11/11
from microbit_radio import *
# Het geheime kanaal en de groep moeten
# hetzelfde zijn als dat van de zender.

kanaal = 1
groep = 1
clear_history()
print("Man-in-the-middle aanval!")
bericht = rx(kanaal,groep)
print("\nBericht =",bericht)
    
```

Extra uitdagingen

- Probeer een andere rol in je groep.
- Voeg een andere groep studenten toe en maak een grote groep chat.
- Probeer de activiteit met hetzelfde kanaalnummer uit te voeren, maar een ander groepsnummer.

Samengevat

- De ontvanger moet luisteren naar het kanaalnummer en dit instellen voordat de zender het bericht verzendt.
- Een radioboodschap kan worden verzonden via een willekeurige combinatie van de 84 radiokanalen of 256 radiogroepen van de micro:bit.
- Om micro:bits te laten communiceren, moeten ze hetzelfde kanaal en dezelfde groep gebruiken.
- Boodschappen die in *cleartext* over een bekend kanaal en groep worden verzonden, kunnen worden gehackt.
- Het gebruik van een geheim kanaal of een geheime groep kan helpen om *hacking* te voorkomen.

Tips voor als het misgaat

- Controleer of iedereen in de groep hetzelfde kanaal- en groepsnummer gebruikt.
- Zorg ervoor dat de ontvanger en hacker hun programma's uitvoeren en wachten voordat de zender het bericht verzendt.