Cybersecurity 1: All Clear
TI-84 Plus CE Python

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-84's 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 x 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 gebundeld in een **pakketje** inclusief informatie over routing en foutcontrole. Dit pakketje wordt vervolgens toegevoegd aan radiogolven wat **digitale modulatie** wordt genoemd.
- Naast radiokanalen van de micro:bit, 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 TI-84 Plus CE Python 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**
        - Open het programma **ONTV_1**, wijzig het het kanaal naar het toegewezen kanaalnummer en run het programma voordat de zender zijn programma uitvoert.

- De **zender**
  - Open het programma **ZEND_1**, bewerk de berichtstring, wijzig het het kanaal naar het toegewezen kanaalnummer en run het programma nadat de ontvanger en hacker hun programma hebben gestart.
- De **hacker**
  - Open het programma **HACK_1**, wijzig het het kanaal naar het toegewezen kanaalnummer en run het programma 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

```
EDITOR: ZEND_1
PROGRAM LINE 0001
from microbit import *
from mb_radio import *
# Length moet groter zijn dan
# het langste bericht.
# Channel en group moeten
# hetzelfde zijn als dat van
# de ontvanger.
radio.on()
disp_clr()
radio.config(length=250, channel
    =12,power=6,group=1)
Fns… | a A # | Tools | Run | Files
```

Ontvanger

```
EDITOR: ONTV_1
PROGRAM LINE 0001
from microbit import *
from mb_radio import *
# Length moet groter zijn dan
# het langste bericht.
# Channel en group moeten
# hetzelfde zijn als dat van
# de zender.
radio.on()
disp_clr()
radio.config(length=250, channel
    =12,power=6,group=1)
Fns… | a A # | Tools | Run | Files
```

Hacker

```
EDITOR: HACK_1
PROGRAM LINE 0001
from microbit import *
from mb_radio import *
# Length moet groter zijn dan
# het langste bericht.
# Channel en group moeten
# hetzelfde zijn als dat van
# de zender.
radio.on()
disp_clr()
radio.config(length=250, channel
    =12,power=6,group=1)
Fns… | a A # | Tools | Run | Files
```

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.

Bestanden

- Zet de onderstaande programma's op je rekenmachine m.b.v. de TI Connect CE software. De link om deze software te downloaden staat hier.
  Telkens je met een nieuw onderdeel begint kun je het beste eerst de gebruikte programma's wissen en daarna de programma's voor het nieuwe ondedeel weer op je rekenmachine zetten.

Naam	Beschrijving
ZEND_1.py	Stuurt een tekstbericht naar een ontvanger
ONTV_1.py	Ontvangt een tekstbericht van een zender
HACK_1.py	"Man-in-the-middle-aanval" tussen zender en ontvanger