Cybersecurity 2: Kanaal Surfen
TI-84 Plus CE Python

Achtergrondinfomatie

Hedy Lamarr 1944

- Hedy Lamarr was een trendy Oostenrijks-Amerikaanse filmactrice en werd opgenomen in de National Inventor's Hall of Fame voor haar werk aan radiofrequentie-hoppende spreidingsspectrum radargestuurde torpedo's die werden gebruikt in de Tweede Wereldoorlog. Haar uitvinding ontving het Amerikaanse patent 2.292.387. Deze methode om radioberichten te verbergen houdt in dat kleine delen van een bericht over verschillende radiofrequenties worden verzonden. De zender en ontvanger stemmen af op een lijst van kanalen die gebruikt zullen worden om het bericht te verzenden en te ontvangen. Wanneer het eerste bit van het bericht op het eerste kanaal in de lijst wordt verzonden, schakelen de zender en ontvanger hun radio's over naar het volgende kanaal op de lijst. Elk bit van het bericht wordt over een ander radiofrequentiekanaal verzonden totdat het gehele bericht is verstuurd. Zolang de lijst van kanalen geheim wordt gehouden voor een hacker, kan het bericht niet gemakkelijk worden onderschept. Deze activiteit genereert de kanaallijst op basis van een privésleutel die gedeeld wordt tussen de zender en ontvanger.

Wat is jouw opdracht?

1. Oefen op het maken van een lijst met kanaalnummers in Python:
    - Elk groepslid moet het programma '**OEFEN_2.py'** openen en uitvoeren. Voer eerste een korte sleutel in.
    - Run het programma nogmaals maar voer nu een lange sleutel in.
    - Bij elke sleutel wordt een kanaallijst aangemaakt. Genereert een korte sleutel of een lange sleutel meer kanalen? Welke kanaallijst zou veiliger zijn?
2. Een bericht sturen met behulp van frequentiehopping spreidingsspectrum:
    - Zorg ervoor dat alle groepsleden hetzelfde groesnummer gebruiken.
    - De ontvanger:
        - Open het programma **'ONTV_2.py'**, verander de groep naar je toegewezen nummer en voer het programma uit **voordat** de zender hun programma heeft uitgevoerd.
    - De zender:
        - Ga naar **'ZEND.py'**, verander de berichtstring en de groep naar je toegewezen nummer, en voer het programma uit **nadat** de ontvanger en de hacker hun programma's hebben gestart.
    - De hacker:
        - Ga naar **'HACK_2.py'**, verander de groep naar je toegewezen nummer en voer het programma uit **voordat** de zender hun programma heeft uitgevoerd.
    - Nadat je team de activiteit heeft uitgevoerd, moet de zender het **bericht** en de **sleutel** wijzigen en de sleutel alleen met de ontvanger delen. Vertel de hacker de nieuwe sleutel niet; **houd deze privé!** Kan de hacker je bericht in leesbare tekst lezen zoals ze deden in de 'All Clear' activiteit?

micro:bit

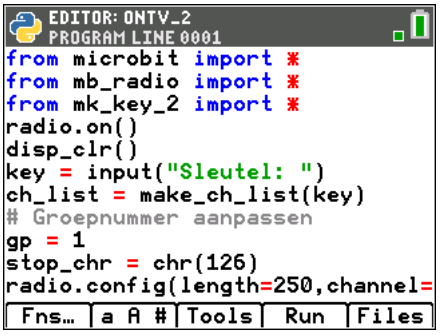
Cybersecurity 2: Kanaal Surfen
TI-84 Plus CE Python

TEXAS INSTRUMENTS

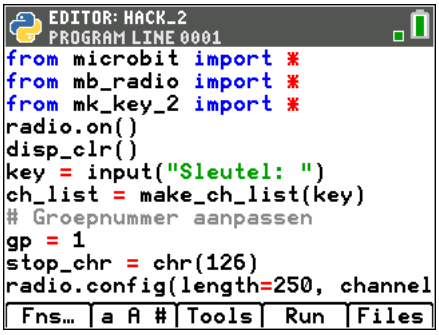
De code

Zender

Ontvanger



Hacker



Extra uitdagingen

- Voer de activiteit opnieuw uit in een andere teamrol.
- Herhaal de activiteit met verschillende sleutels en berichten.
- Probeer te ontdekken hoeveel kanalen er op de lijst staan voor een gegeven sleutel.

Samengevat

- Om te kunnen communiceren, moeten twee radio's op hetzelfde kanaal en dezelfde groep zitten.
- Een zendprogramma kan het kanaal wisselen na het verzenden van elk teken.
- Een ontvangend programma moet van tevoren weten welke kanalen de zender zal gebruiken om het bericht te versturen.
- Het gebruik van een frequentiehopping-algoritme, zoals het algoritme in deze activiteit, kan het hacken moeilijker maken.

Tips voor als het misgaat

- Controleer of iedereen in het team hun toegewezen groepsnummer gebruikt.
- Zorg ervoor dat de ontvanger en hacker hun programma's uitvoeren en wachten voordat de zender het bericht verstuurt.
- Zorg ervoor dat de zender en ontvanger dezelfde sleutel gebruiken.
- Zorg ervoor dat de hacker de sleutel kent.

Cybersecurity 2: Kanaal Surfen
TI-84 Plus CE Python

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 als 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
OEFEN_2.py	Oefenen met het maken van een lijst met kanalen gebaseerd op een private sleutel.
ZEND_2.py	Zenden van een tekst bericht naar een ontvanger met gebruikmaking van frequentie hoppen.
ONTV_2.py	Ontvangen van een tekst bericht naar een ontvanger met gebruikmaking van frequentie hoppen.
HACK_2.py	Ontvangen van een versleuteld bericht.
mk_key_2.py	Hulpprogramma voor de andere vier programma's. Hiermee wordt een lijst met kanalen gemaakt.