So funktioniert es

Hedy Lamarr 1944

Hedy Lamarr war eine angesagte österreichisch-amerikanische Filmschauspielerin und wurde für ihre Arbeit an einem Frequenzsprung-Verfahren zur Steuerung funkgesteuerter Torpedos im Zweiten Weltkrieg in die National Inventor's Hall of Fame aufgenommen. Für ihre Erfindung erhielt sie das US-Patent 2.292.387. Bei dieser Methode zum Verbergen von Funknachrichten werden kleine Teile einer Nachricht auf verschiedenen Funkkanälen übertragen. Sender und Empfänger einigen sich auf eine Liste von Kanälen, die zum Senden und Empfangen der Nachricht verwendet werden sollen. Wenn das erste Bit der Nachricht auf dem ersten Kanal in der Liste übertragen wird, schalten Sender und Empfänger ihre Funkgeräte auf den nächsten Kanal in der Liste um. Jedes Bit der Nachricht wird über einen anderen Funkkanal gesendet, bis die gesamte Nachricht gesendet wurde. Die Nachricht kann nicht leicht abgefangen werden, wenn die Liste der Kanäle vor einem Hacker geheim gehalten wird. Bei diesem Verfahren wird die Kanalliste anhand eines privaten Schlüssels erstellt, den Sender und Empfänger gemeinsam nutzen.

Was ist zu tun?

1. Üben Sie, eine Python-Liste zu erstellen:
    a. Öffnen Sie die Datei *CyberSecurity – Kanalsurfen.tns*
    b. Jedes Gruppenmitglied ruft die Seite mit "**practice_short_key.py**" auf und das führt Programm aus.
    c. Wechseln Sie zur Seite '**practice_long_key.py**'.
    d. Diese beiden Programme erstellen jeweils eine Kanalliste, die vom Schlüssel abhängt. Worin besteht der Unterschied zwischen den Ausgaben der beiden Programme? Erzeugt ein kurzer Schlüssel oder ein langer Schlüssel mehr Kanäle? Welche Kanalliste wäre sicherer?
2. Senden einer Nachricht mit Frequenzsprungverfahren:
    - Der *Empfänger*:
        - wechselt zu "**student_receiver.py**", ändert den Kanal auf die zugewiesene Nummer und führt das Programm aus**, bevor** der *Sender* sein Programm ausgeführt hat.
    - Der *Sender*
        - wechselt zu "**student_sender.py**", ändert den Kanal auf die zugewiesene Nummer und führt das Programm aus**, nachdem** der *Empfänger* und der *Hacker* ihre Programme gestartet haben.
    - Der *Hacker*
        - wechselt zu "**student_hacker.py**", ändert den Kanal auf die zugewiesene Nummer und führt das Programm aus**, bevor** der *Sender* sein Programm ausgeführt hat.
    - Nachdem Ihr Team die Aktivität ausgeführt hat, ändert der *Sender* die **Nachricht** und den **Schlüssel** und gibt den Schlüssel nur an den *Empfänger* weiter. Teilen Sie dem *Hacker* den

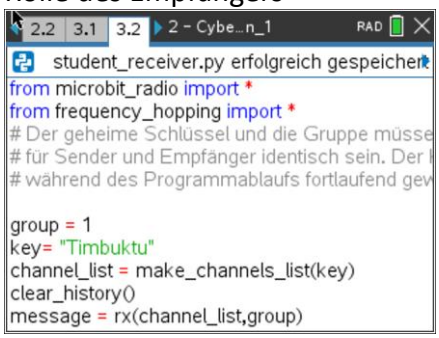
©Texas Instruments 2024

neuen Schlüssel nicht mit; **behalten Sie ihn für sich**! Kann der *Hacker* Ihre Nachricht im Klartext lesen, so wie er es in der "All Clear"-Aktivität getan hat?

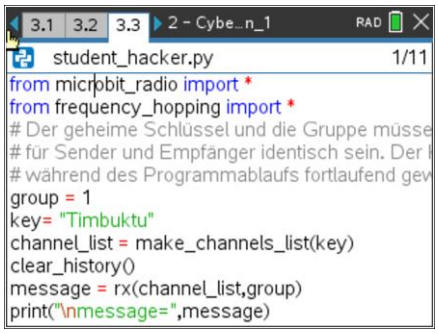
Die Programme

Rolle des Senders

Rolle des Empfängers



Rolle des Hackers



Weitere Übungen

- Wiederholen Sie die Aktivität in einer anderen Teamrolle.
- Wiederholen Sie die Aktivität mit anderen Schlüsseln und Nachrichten.
- Versuchen Sie herauszufinden, wie viele Kanäle in der Liste für einen bestimmten Schlüssel stehen.
- Wie können Sie die Anzahl der Kanäle ändern? Ist eine lange oder kurze Liste sicherer?
- Versuchen Sie, die Nachricht schneller zu übermitteln. Was passiert, wenn sie zu schnell ist?

Prüfen Sie Ihr Verständnis

- Damit mehrere *micro:bits* miteinander kommunizieren können, müssen sie sich auf demselben Kanal und in derselben Gruppe befinden.
- Ein sendendes Programm kann den Kanal nach jedem Zeichen umschalten.
- Ein empfangendes Programm muss die Kanäle, die der *Sender* zum Senden der Nachricht verwendet, im Voraus kennen.
- Die Verwendung eines Frequenzsprung-Algorithmus, wie in dieser Aktivität benutzt, kann das Hacken erschweren.

Hilfe

- Vergewissern Sie sich, dass alle Teammitglieder die ihnen zugewiesene Gruppennummer verwenden.
- Stellen Sie sicher, dass der *Empfänger* und der *Hacker* ihre Programme starten und warten, bis der *Sender* die Nachricht übertragen hat.
- *Empfänger* und *Hacker* können ihre Programme bei Bedarf durch Drücken der <esc> Taste jederzeit beenden.
- Stellen Sie sicher, dass *Sender* und denselben Schlüssel verwenden.
- Stellen Sie sicher, dass der *Hacker* den Schlüssel kennt.

©Texas Instruments 2024