# Raspberry Pi Security Project: Blocking the Replay Attack

Joshua Klotzkin
Masters' Student
Computer Science Department
Binghamton University
Binghamton, NY 13902-6000

## Project goals

The replay attack is when a video stream is interrupted and previously recorded video is inserted. This masks what is currently happening in the view of the camera. Such attacks can compromise security monitoring. This is used in the movie "Oceans Eleven."

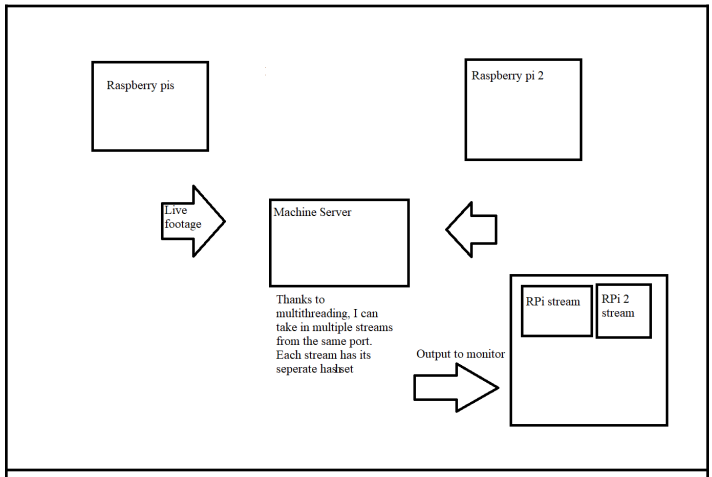


Figure 1: Block diagram of system, showing two Raspberry Pis, and a central monitoring computer. The Raspberry Pis can simulate replay attacks and the central monitoring computer will detect the attack and warn the user.

The goal of the current project is to stream video footage from multiple Raspberry Pis onto a single machine, and detect replay attacks and repeated footage, so as to be a more accurate security system. In order to test the system, the Raspberry Pis must simulate replay attacks for the machine server to detect.

## Project Method:

I have created a receiver to be run on a machine and act as a server and a sender with camera software to be run on Raspberry Pis and act as a client. The user will run the server first, and the server will wait until a client is run and connected. Once the sender starts running the user is prompted to type in the ip address of the server.

Once they are connected the client will stream footage from the camera. The handle clients function allows for multithreading through the same port so it can handle multiple streams at once, by wrapping each stream in a file object for easier reading and streaming of incoming frames. The file also stores the hash sets of that individual camera.

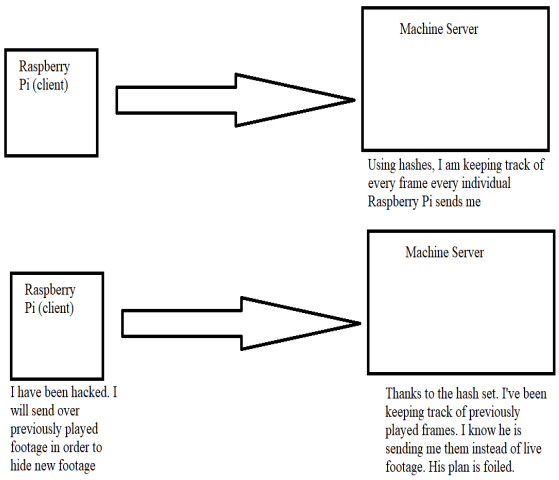


Figure 2: The system works as follows. As the Raspberry Pi client sends video, the server creates a hash of every video frame that will identify it hopefully uniquely. If the server detects ten frames with a hash already in the database in a row, it flags the footage as a loop.

The receiver is designed to prevent replay attacks by creating a hash set per thread and if it detects a certain amount of frames in a row with an identical hash set it will display a Loop Detected text on the screen. The hash set doesn't take up much data, as running it for 10 minutes only generated 1.3 kB of Data

In order to test this, the current clients can record footage with the space bar and stream the recorded footage to the server with the press of the L button. This will send the recorded footage instead of the current footage and should be flagged as a loop in the server.

## Pictures and Figures:

Below shows an example. The first picture was sent originally while I was pressing the space bar. The second picture, when I pressed the “L” to insert the captured footage, is flagged as looped footage by the server.


Recording normally

Detecting a loop attack on the server

Figure 3: Pictures taken from the server side. The first is original footage, the second looped footage sent by the Raspberry Pi.

Python Implementation Details: The Pi currently uses Opencv in order to stream and record video footage. In the future we will implement YOLO in order to detect whether or not a person is on screen.

Conclusion: A Raspberry Pi security system that blocks replay attacks was successfully implemented using a hash set to detect repeated frames. The next part of the project, should I choose to work on it, will involve face detection during replay attacks.Thank you for the opportunity to develop this application.