Diogo Ferreira *76504*
Davide Leira *76514*

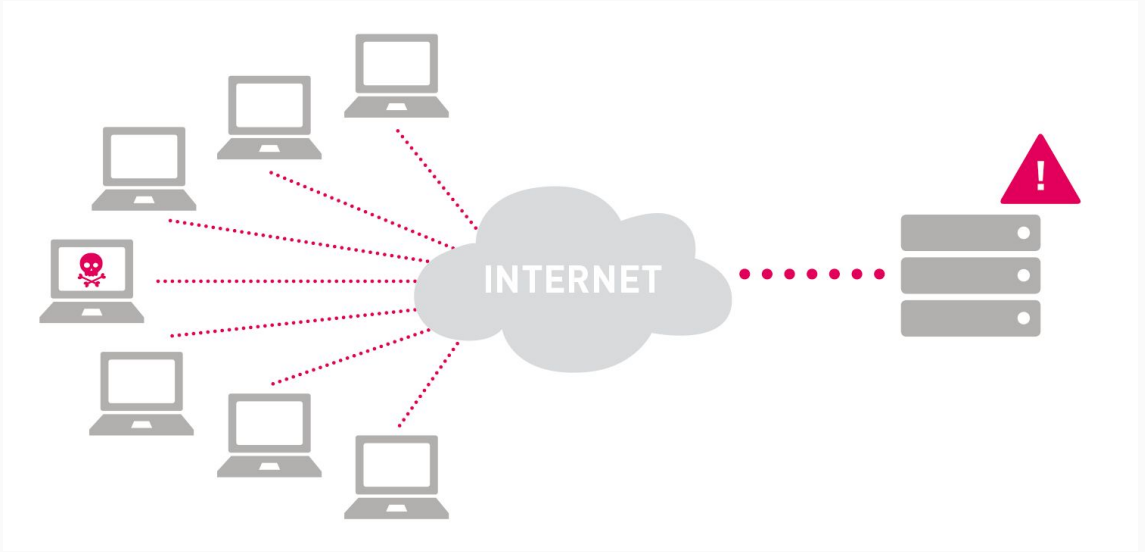
Computação Reconfigurável

FPGA real-time DoS attack monitoring

in a 5G network

What is a *DoS attack*?

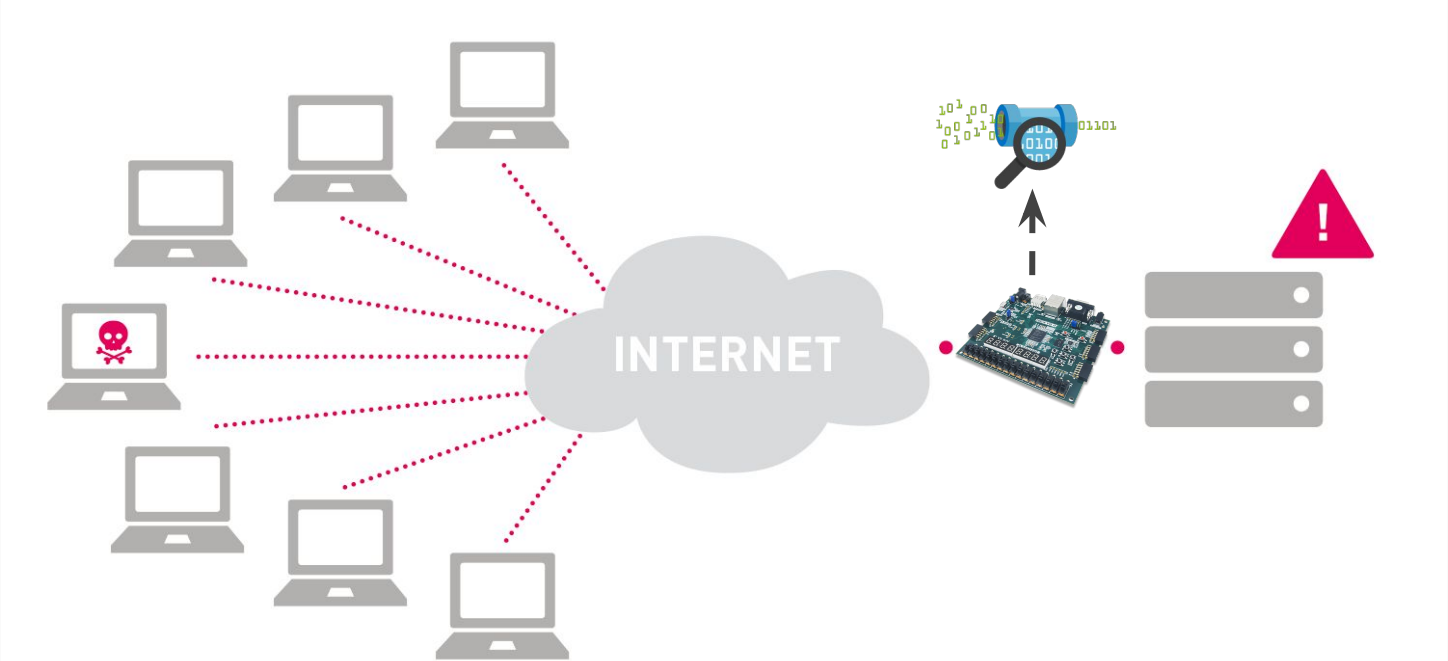
- Large traffic flooding a host, disrupting the network and the service.



System features

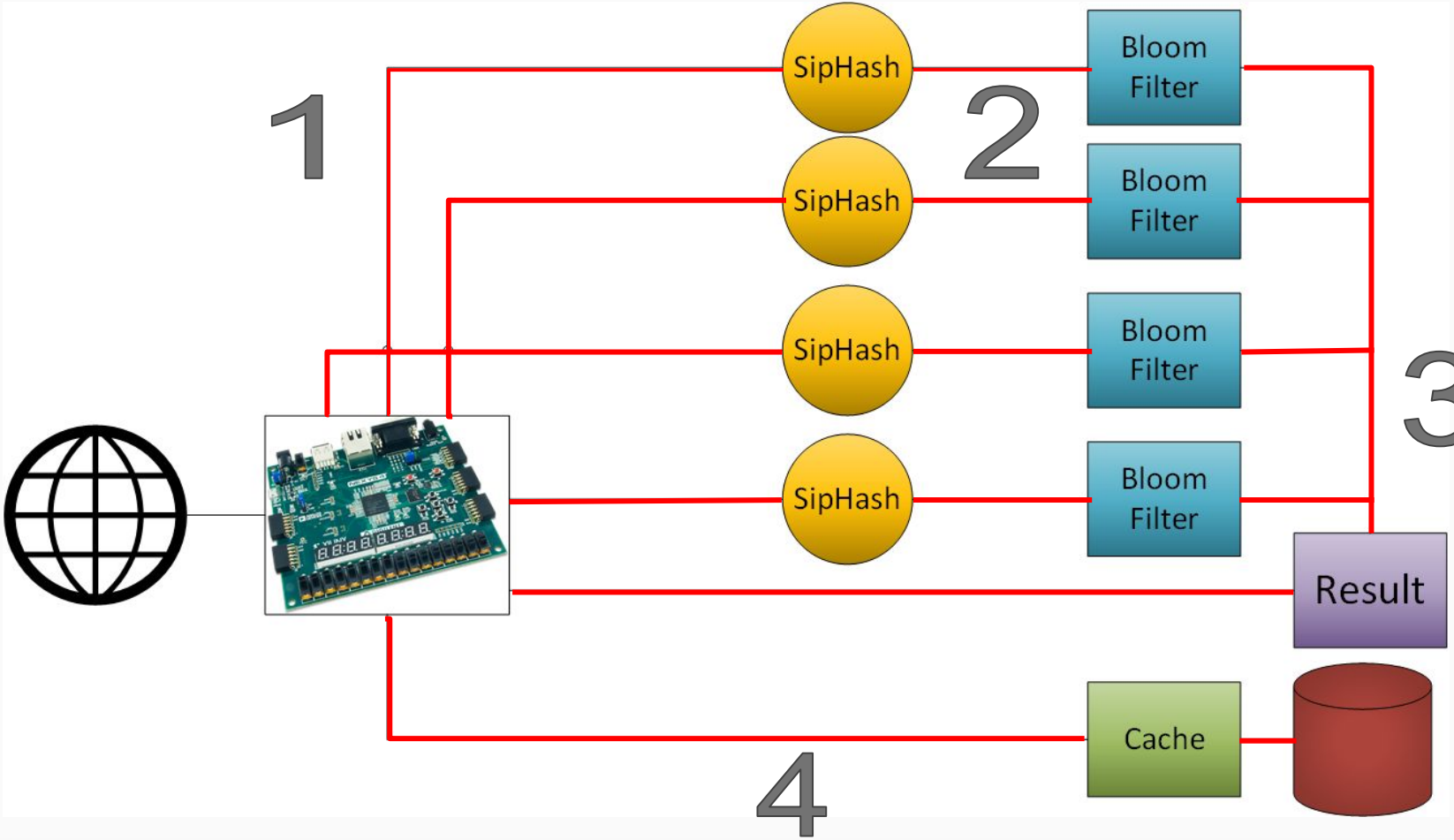
- Receive and analyze IP packets, checking if its source IP is in the blocked IPs blacklist and if it is currently occurring a *DoS attack*.
- Count all received packets and packets from blocked IPs. The first count is shown on the first four displays and the second in the remaining ones.
- Two RGB leds indicate if the last packet is from a blocked IP (red/green) and show a red/green range of colors according to the percentage of packets received from blocked IPs.
- Button to reset the packet counters.

How is the monitoring done?



(Simplistic) *DoS attack* detection

- Circular buffer with source IPs of the last N received packets.
- Every X seconds (triggered by a timer interrupt) clear the buffer.
- If all IPs on the buffer are equal, add IP to blacklist.


SipHash
SipHash
SipHash
SipHash
Bloom Filter
Bloom Filter
Bloom Filter
Bloom Filter
1
2
3
4
5
Result
Cache

SipHash

- It is a family of fast short-input pseudorandom functions.
- It is used in network traffic authentication and defense against hash-flooding DoS attacks: *“Secure, Fast and Simple”*.
- VHDL implementation runs at a maximum frequency of 44.65 MHz (needs slower clock from system clock).

Presented in *SipHash: a fast short-input PRF (2012)* by Aumasson, Jean-Philippe & Bernstein, Daniel.
Implemented in VHDL by Pedro Brito *(https://131002.net/siphash/)*

Bloom filter

- With the input of the hash, check whether the calculated hash was already written.
- False positives are possible (but probability is low).
- Used as a fast method to see if an IP was written to memory. If the result is positive, it is needed a memory access to confirm the decision.

Cache memory

- It contains a cache with at most the last 32 IPs.
- When the cache becomes full with 32 new IPs, the block is written into memory - write-back policy.
- When reading, first checks if the IP is in cache. If it is not, it reads memory blocks one by one and check if the IP is in any of them.

External memory

- Buffer in cellular ram emulates an external memory.

- The transfers between the internal and external memory are done through the CDMA (*Central Direct Memory Access*) controller, which does a memory-mapped to memory-mapped transfer.

Displays and RGB leds

- Each one is controlled by two peripherals.
- The displays are used to show packet counts.
- The RGB leds are used to show the relative amount of packets from blocked IPs and the result of the last packet verification.

Diogo Ferreira *76504*
Davide Leira *76514*

Computação Reconfigurável

FPGA real-time DoS attack monitoring

in a 5G network