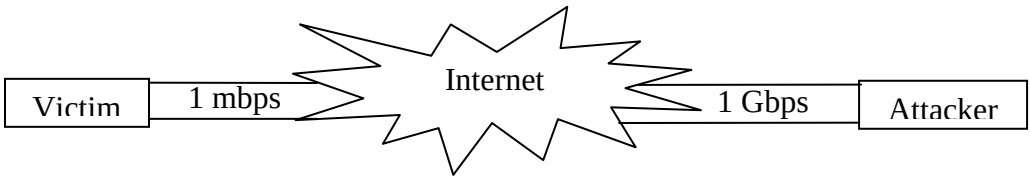
DOS

Denial of Service Attacks

-Crashing the Program
=>Resource Exhaustion
  -Network Bandwidth
  -memory
  -OS resources
  -Disk
  -CPU

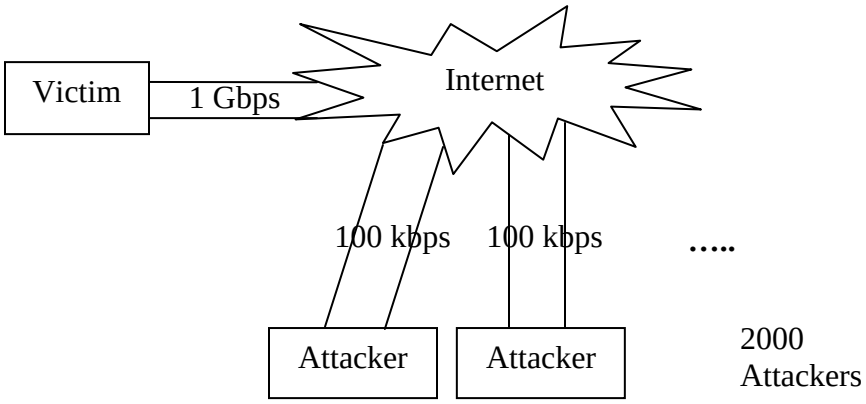
The Using Client Puzzles to Protect TLS paper is an attack on the CPU.

Some Network DOS Attack



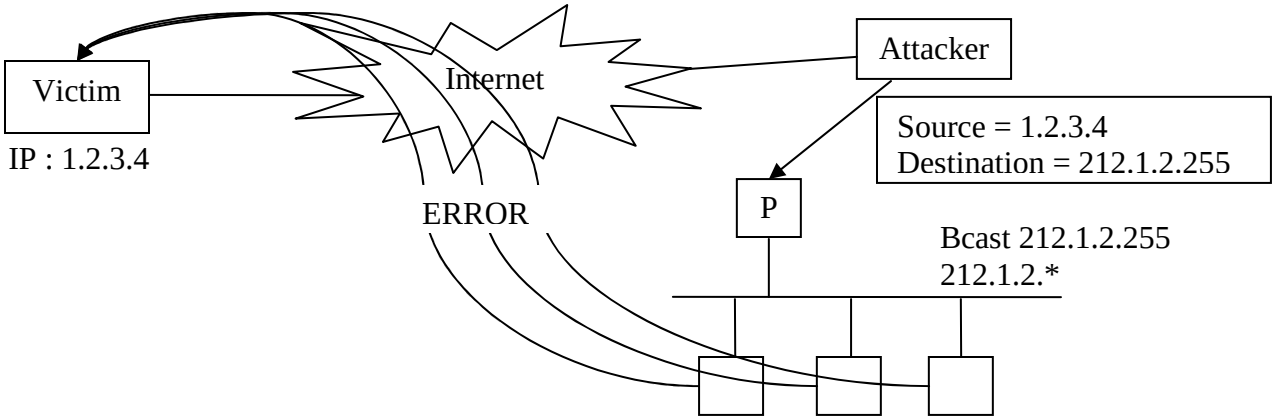
The attacker does not care about being caught.
Usually it is the victim who has a larger bandwidth.

Now Distributed Attack



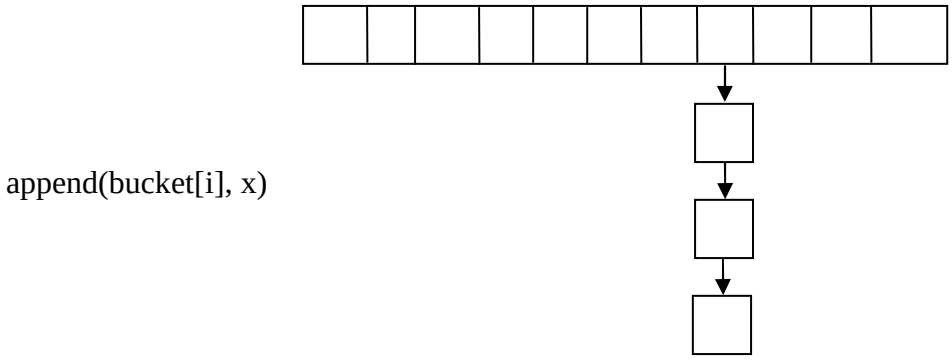
-More attacker machines harder to distinguish attackers.

SMURF Attack



CPU DOS

-Algorithmic Complexity Attacks
Example : Hash Tables
i = hash (x)

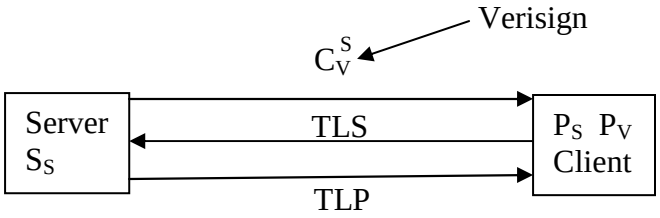


-hash function is typically fixed and public
=>easy for an attacker to find collisions

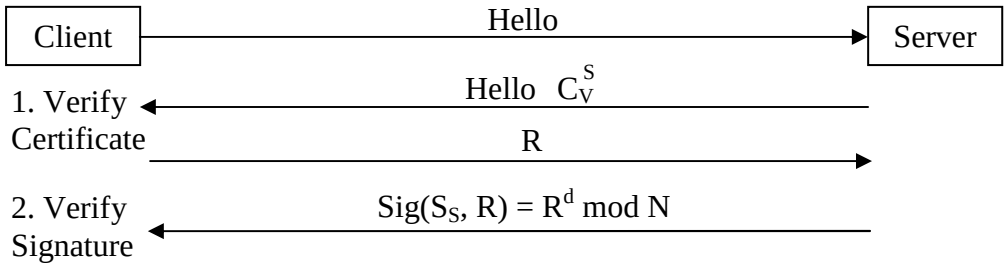
Attack

1. Choose many inputs that all hash to 0.
2. Interact with server to cause it to insert X_1, …, X_n into its hash table
3. Force server to do hash table look ups

TLS / SSL

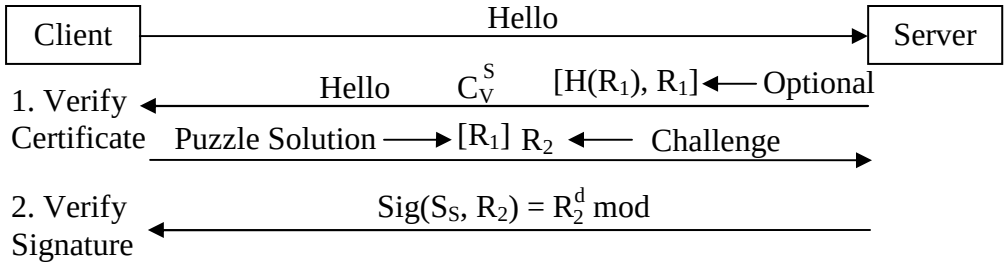


TLS guarantees
-secrecy
-authenticity
-server identity



-modular exponentiation is slow
-typical desktop ≈ 100 signature / second

Client Puzzles



Problems

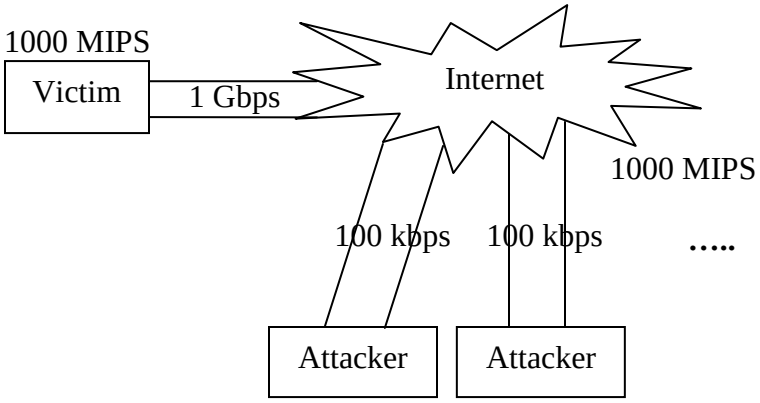
-Doesn't distinguish real overload of the site from attacks
-Must be configured as to when the server starts and ends puzzle request. In the paper they kind of chose to stop requesting puzzle at an arbitrary point.
-Discriminates again slow clients

CPU puzzles vs. Memory Puzzles

Top end Machine	3GHz	2GB
Phone	.1GHz	128MB
	30	16

Not getting a whole lot by switching from CPU to memory such that will not discriminates against slow clients.

The attacker can use his bot net to help compute the puzzle quickly and still cause DOS on the server.



The puzzle's goal is to forces the attacker to have greater resource than victim.