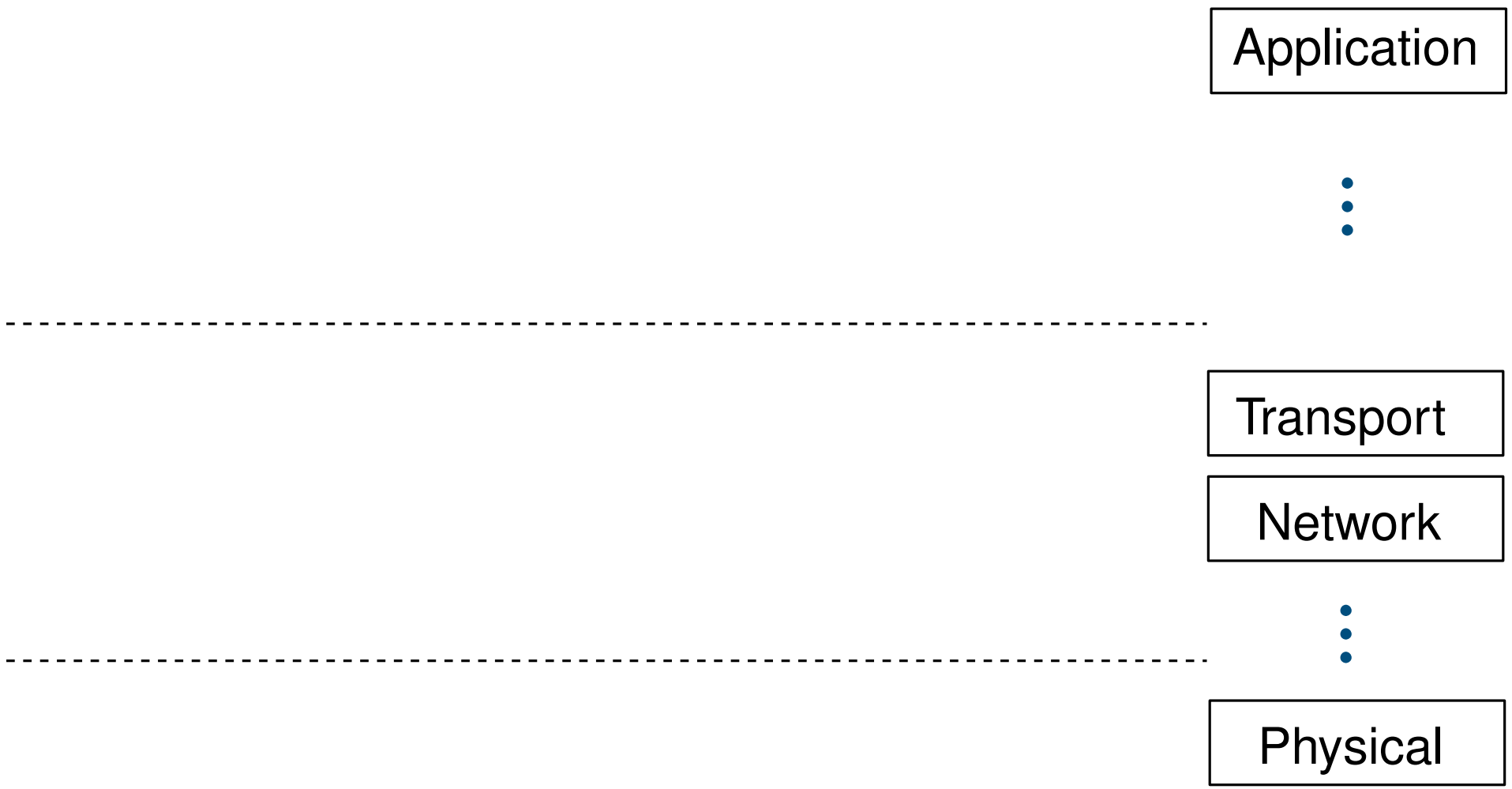
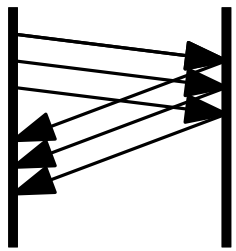
SeVen: A Selective Defense for Low-Rate Application Layer DDoS Attacks

Vivek Nigam
Networking Laboratory
Federal University of Paraíba - UFPB

Application-Layer DDoS Attacks



Application-Layer DDoS Attacks



TCP SYN Flood

- High traffic loads;
- Affects all services;
- Effective mitigation mechanisms

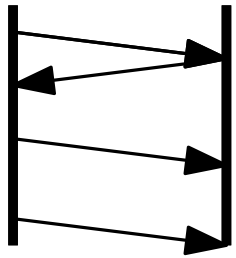
Application

Transport

Network

Physical

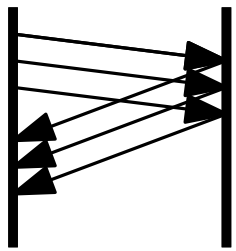
Application-Layer DDoS Attacks



Slowloris / POST

- Small traffic loads: one computer can shut down a web-server;
- Traffic similar to legitimate clients;
- Can target a single service leaving the remaining sevices undisturbed;
- Tools available for carrying out attacks and very simple to use (even by amateurs);
- Few defenses: IP filters, deny services to slow clients, etc.

Application



TCP SYN Flood

- High traffic loads;
- Affects all services;
- Effective mitigation mechanisms

Transport

Network

Physical

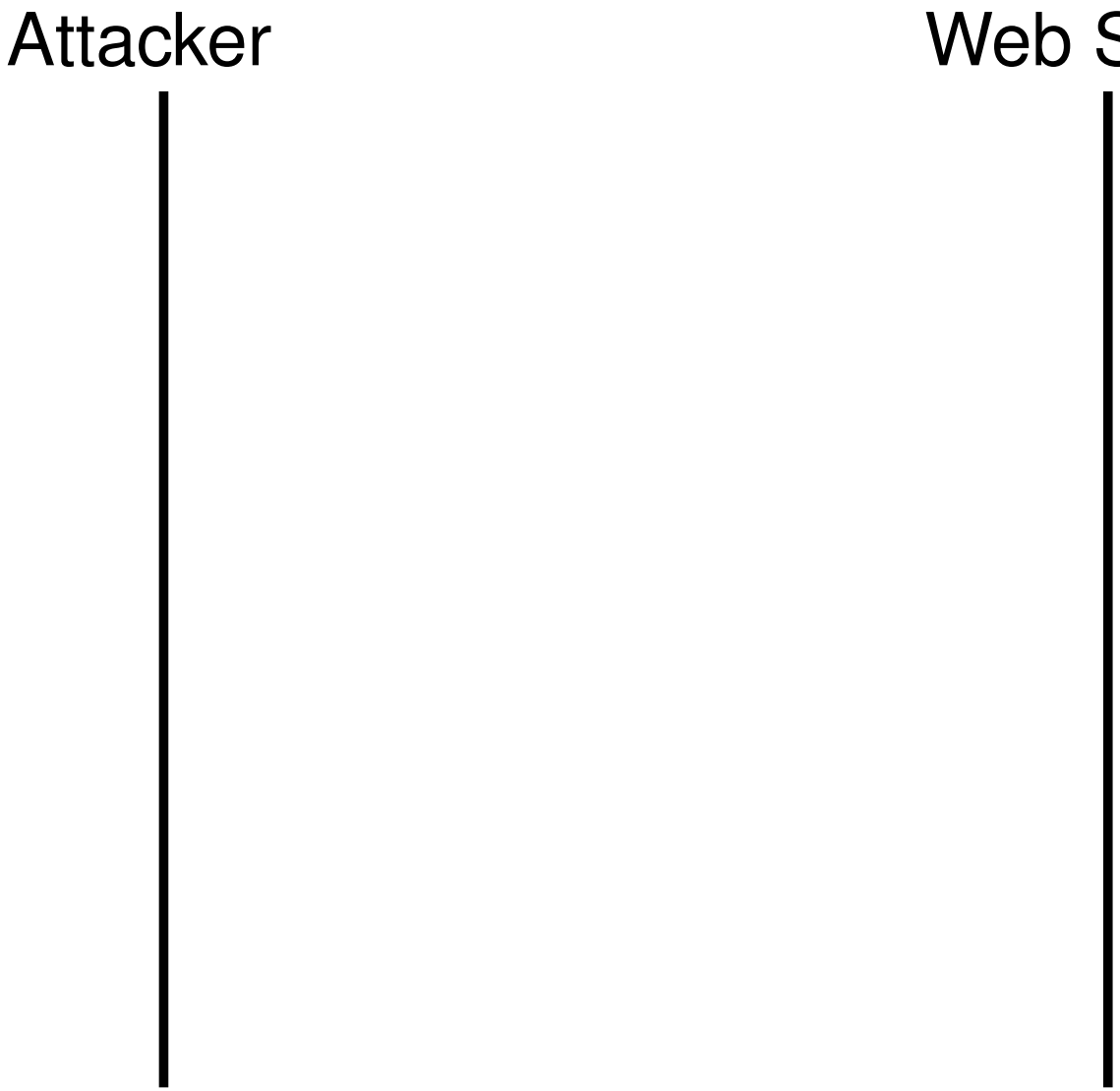
Application-Layer DDoS Attacks

- In 2013, **37.2% of all** DDoS exploited the HTTP protocol.

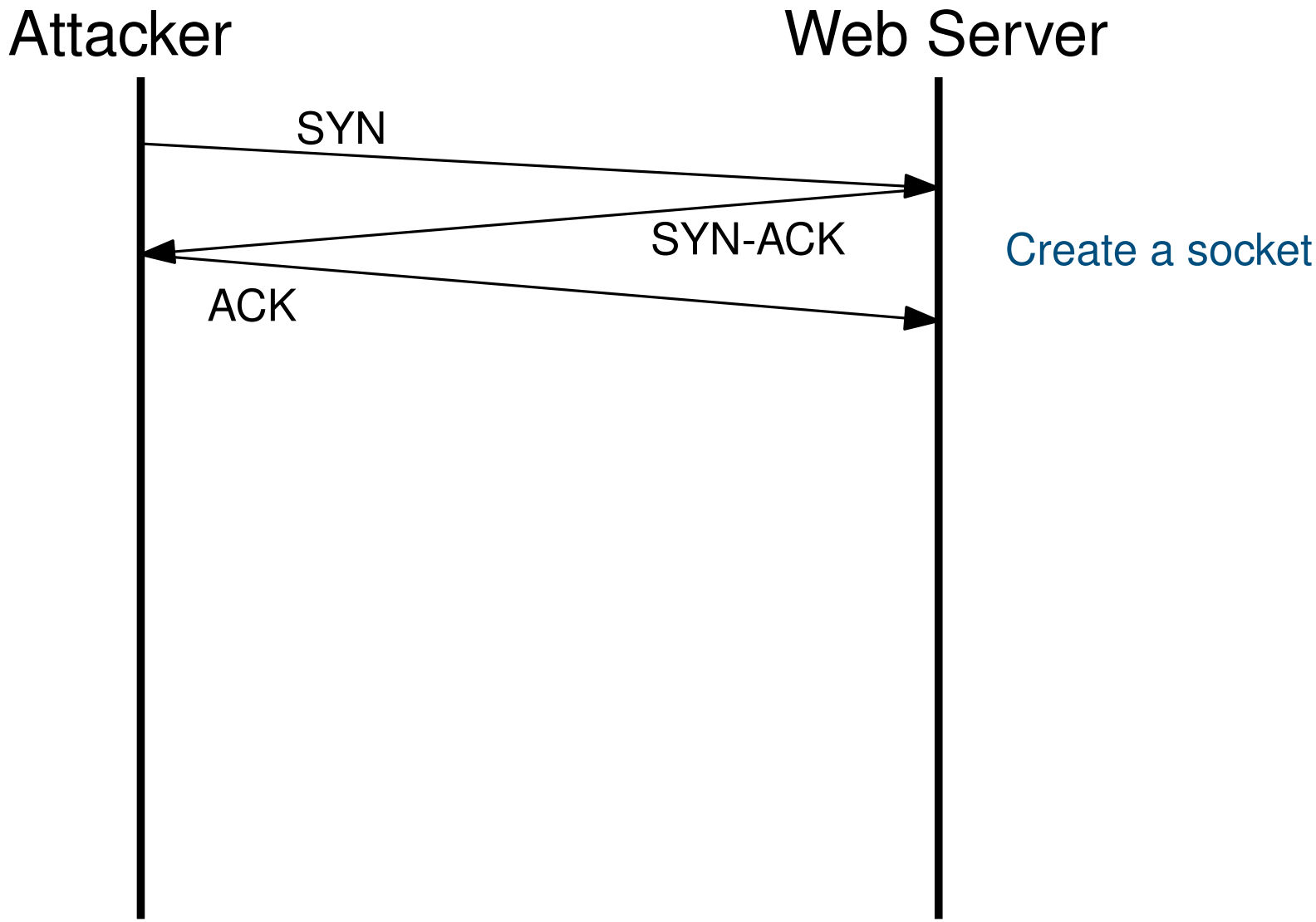
> "Profit-driven cybercriminals pay much closer attention to hackernomics, using the **least amount of resources** to cause the **maximum damage** or disruption to victims. This is why we should **expect application layer attacks to become the most prevalent attacks now and in the future.**"

Source: http://www.nsfocus.com/SecurityReport/

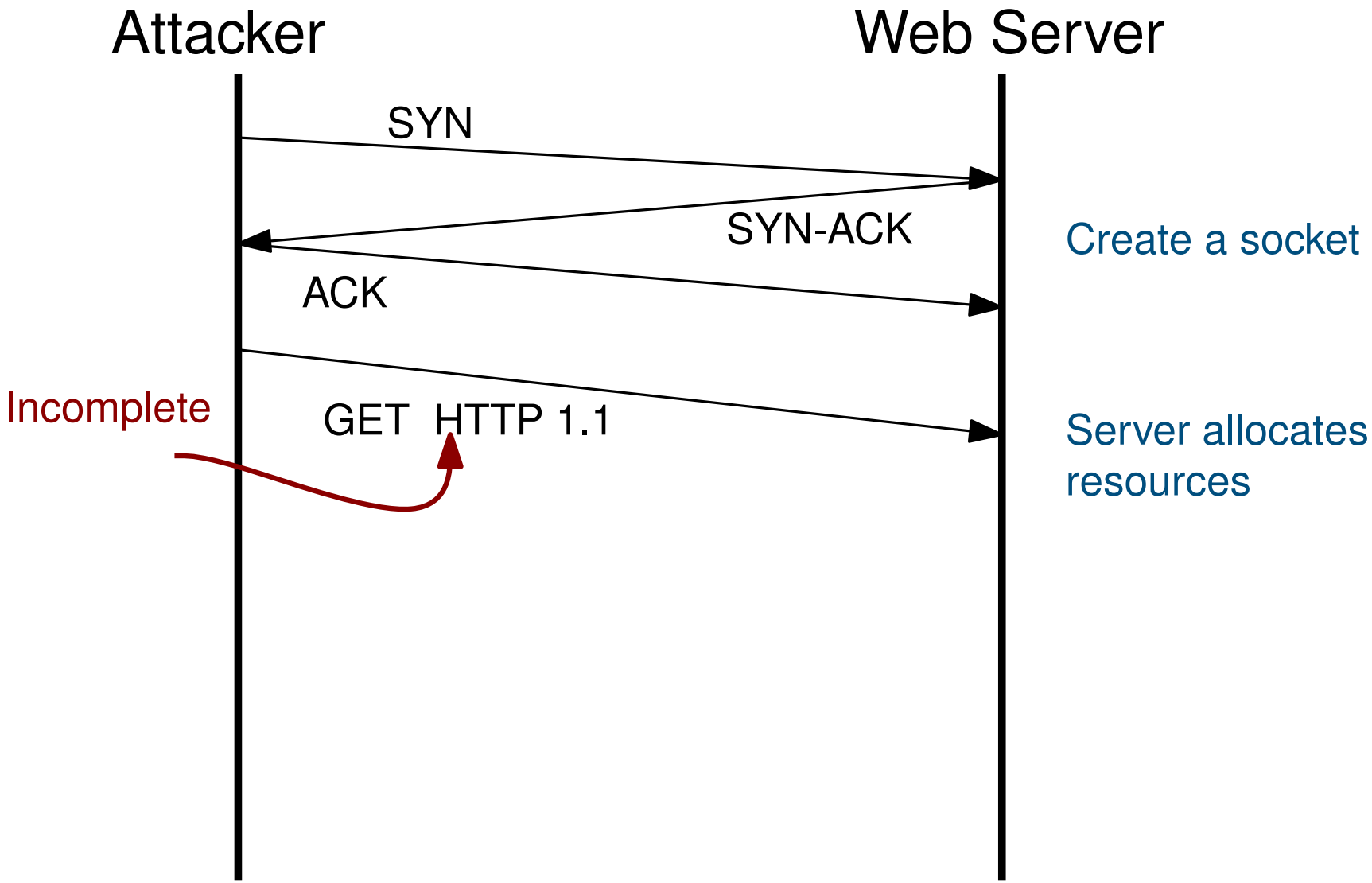
Slowloris Attack



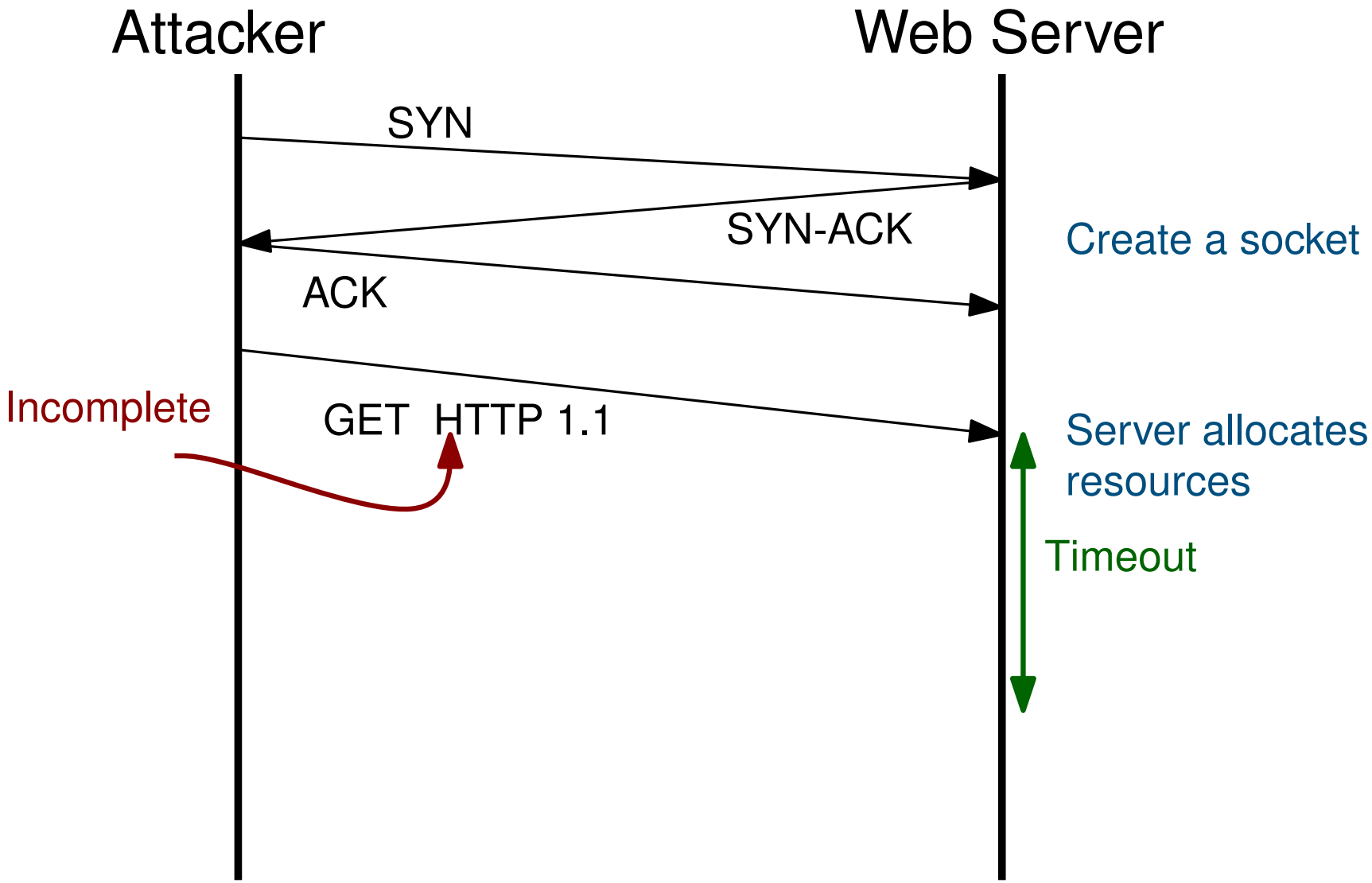
Slowloris Attack



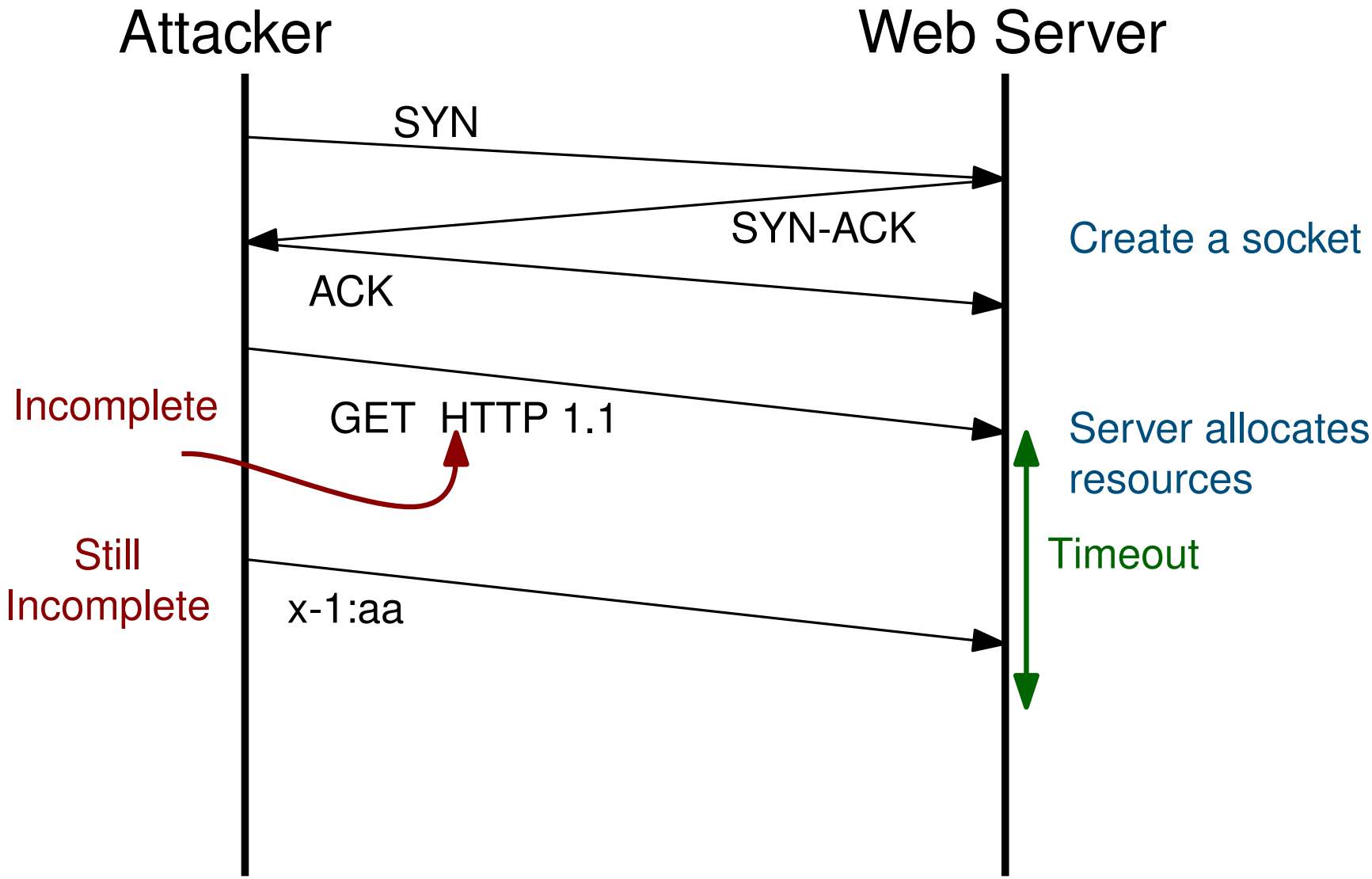
Slowloris Attack



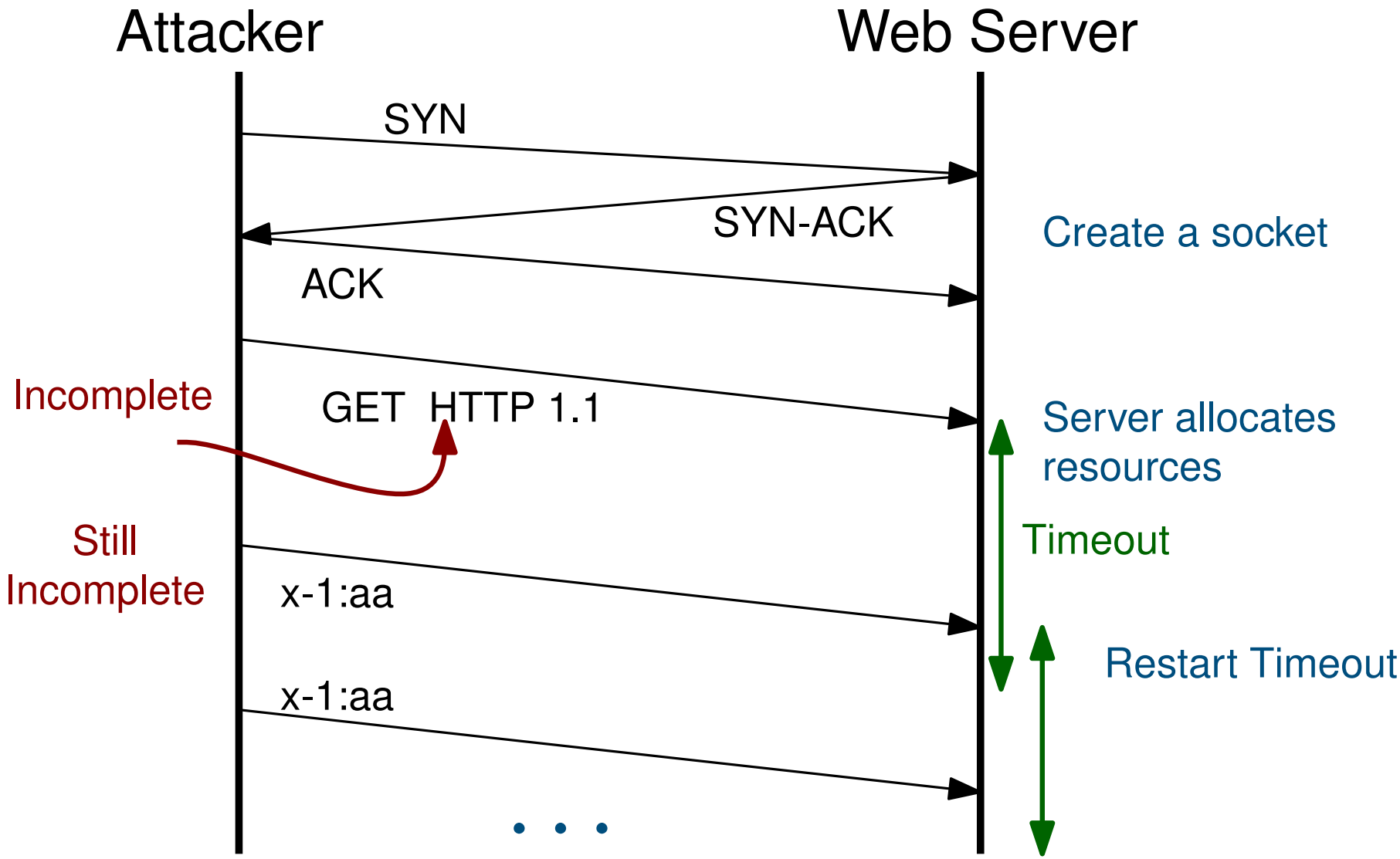
Slowloris Attack



Slowloris Attack

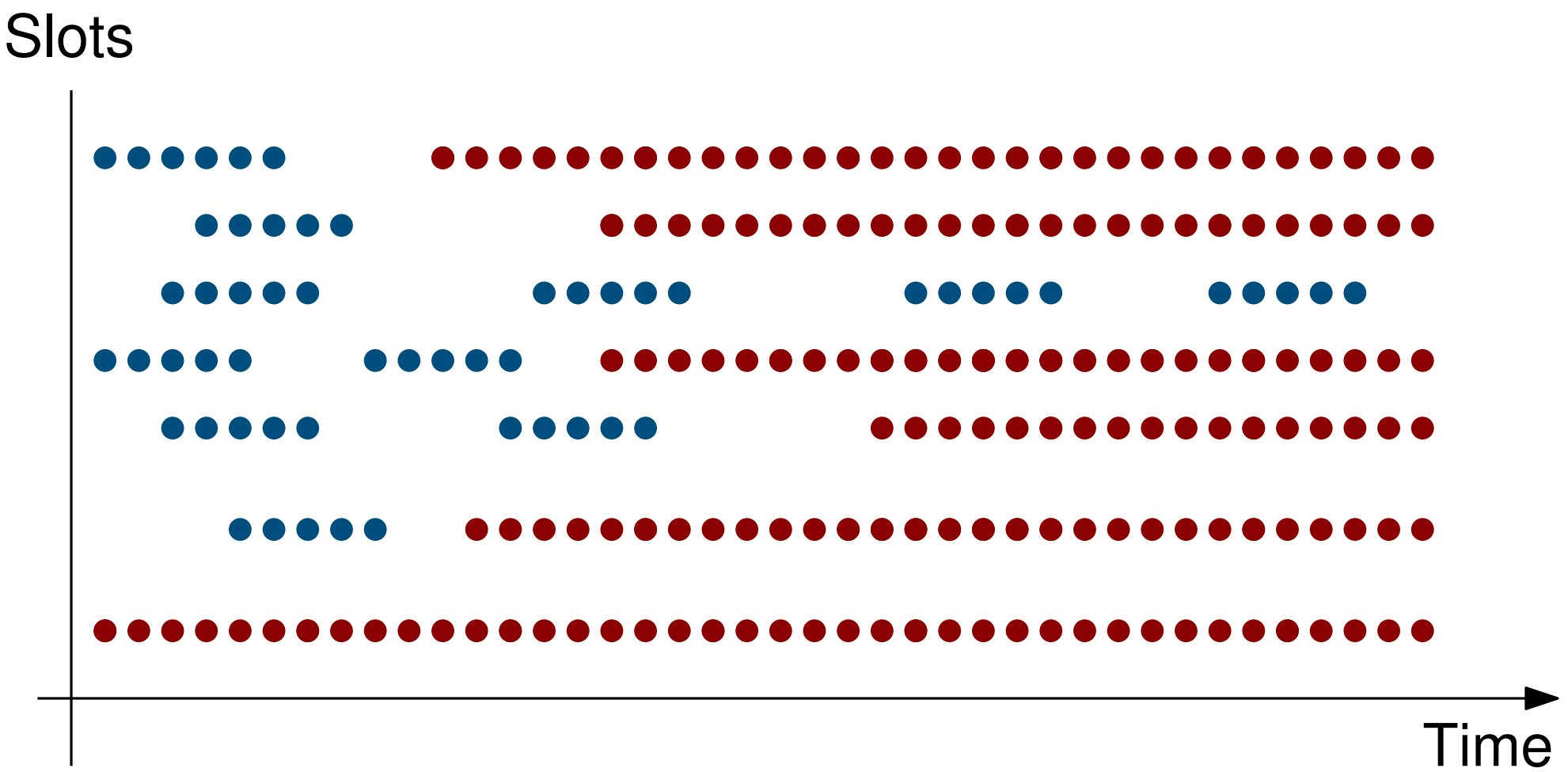


Slowloris Attack

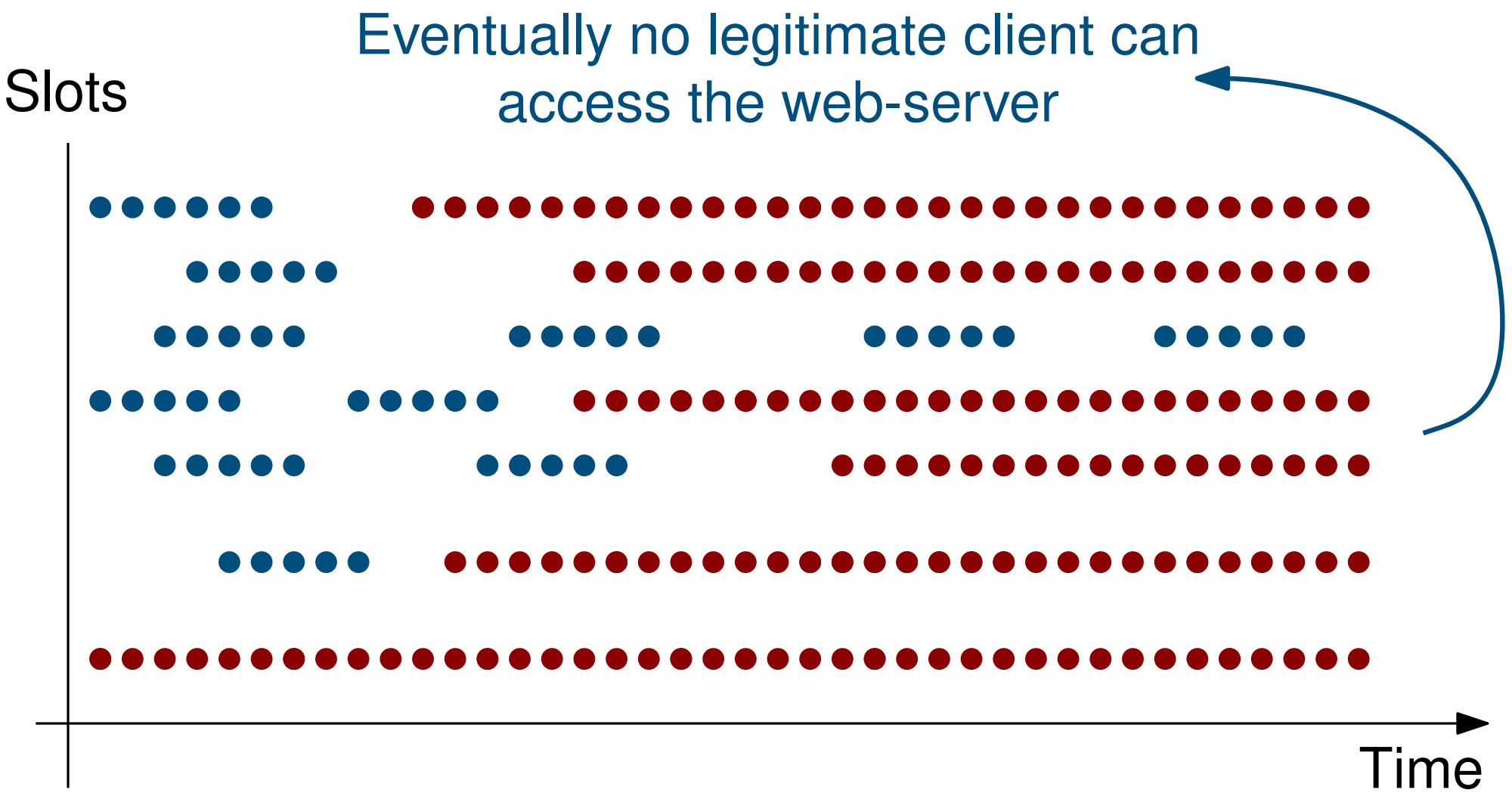


Fatal for connection based web-servers such as Apache.

Why are these attacks so effective?



Why are these attacks so effective?



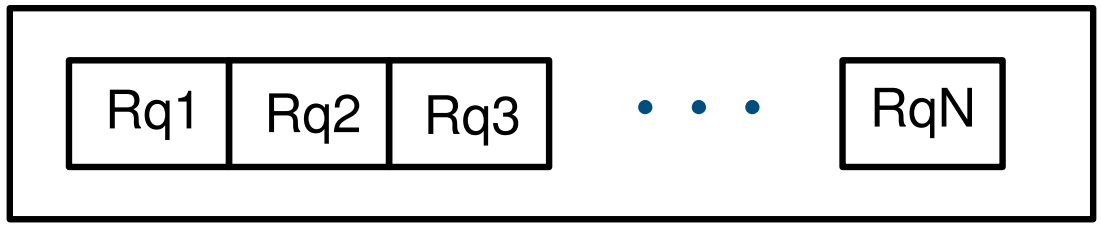
Other Attacks

- **POST** (also know as RUDY - R You Dead Yet)
- **SlowRead** (also **effective on event based webservers such as NGinx**)
- **GET Flood** (**high traffic load**)

SeVen - Selective Verification Defense

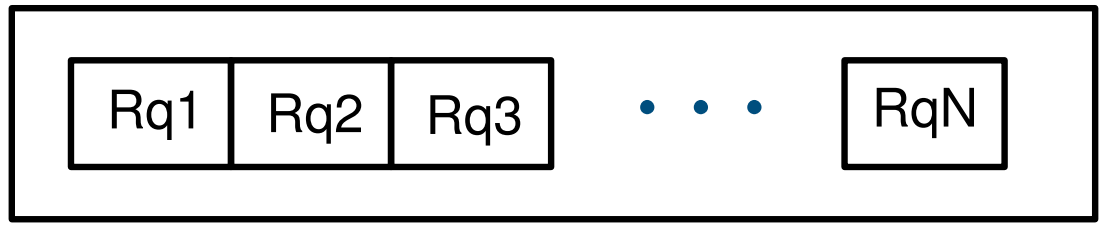
SeVen - Selective Verification Defense

- Monitor **the number of established connections** with the server.

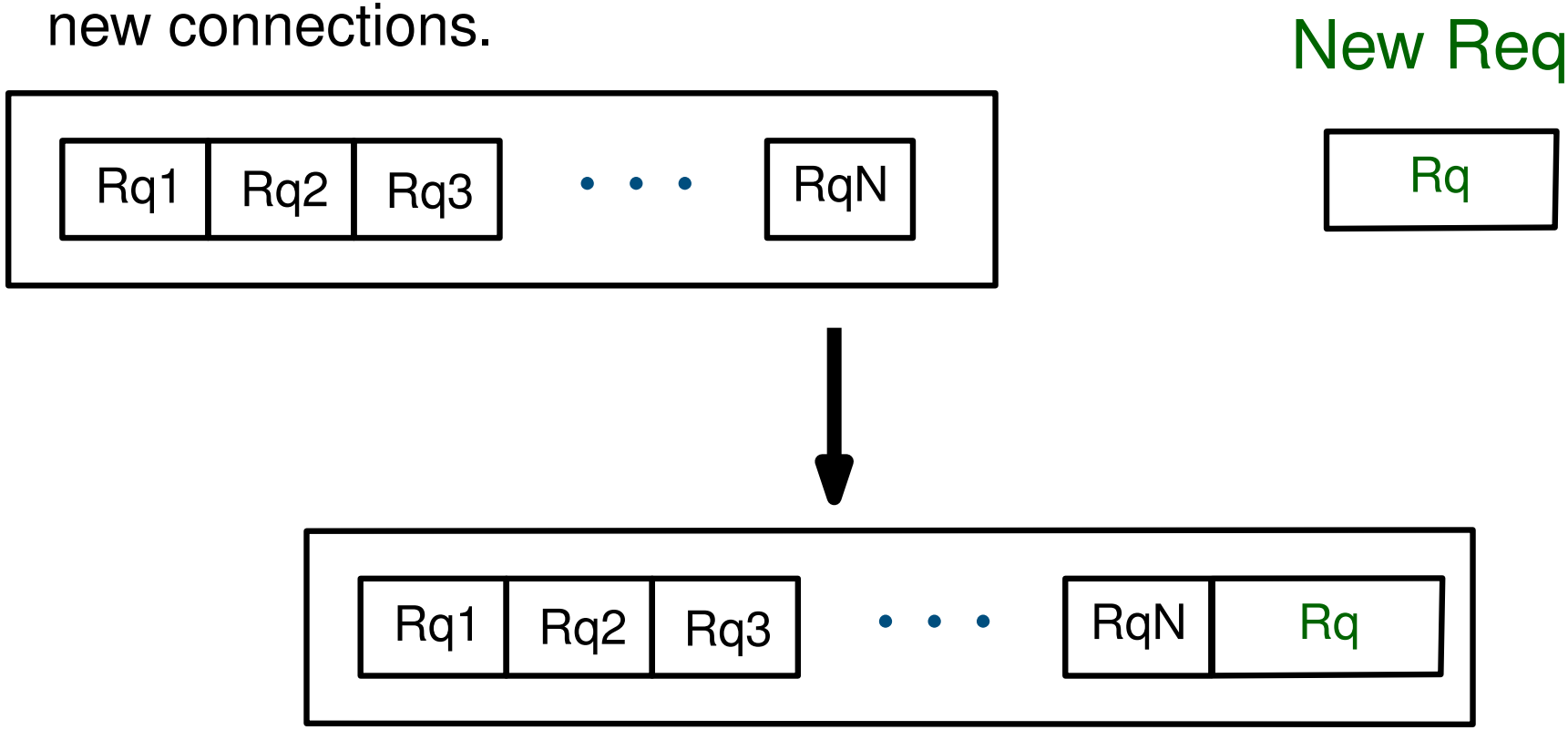


SeVen - Selective Verification Defense

- Monitor **the number of established connections** with the server.

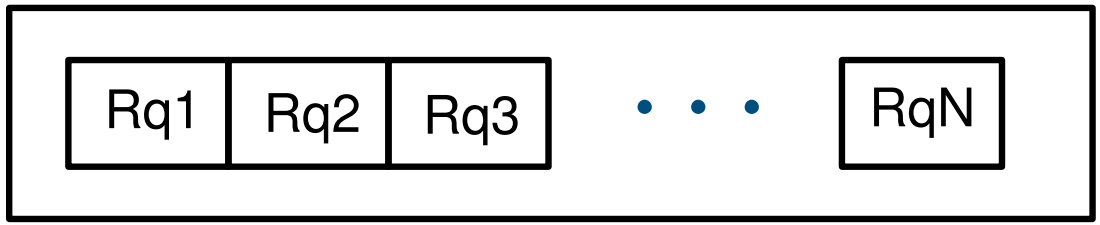


- If **N less than the máximum number** of connections, then accept new connections.



SeVen - Selective Verification Defense

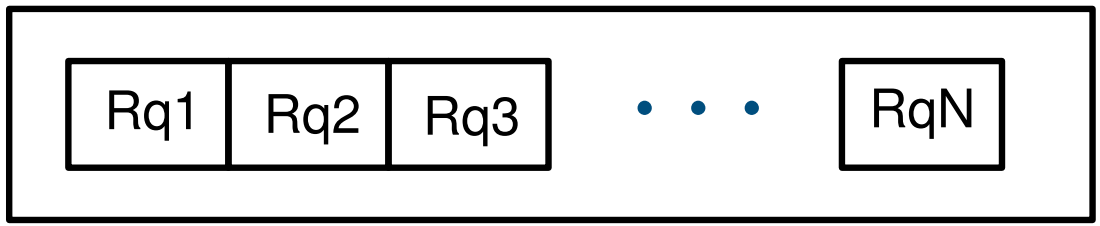
- If **N is equal to the maximum number** of connections, then select requests:



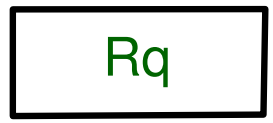
New Req

SeVen - Selective Verification Defense

- If **N is equal to the maximum number** of connections, then select requests:



New Req



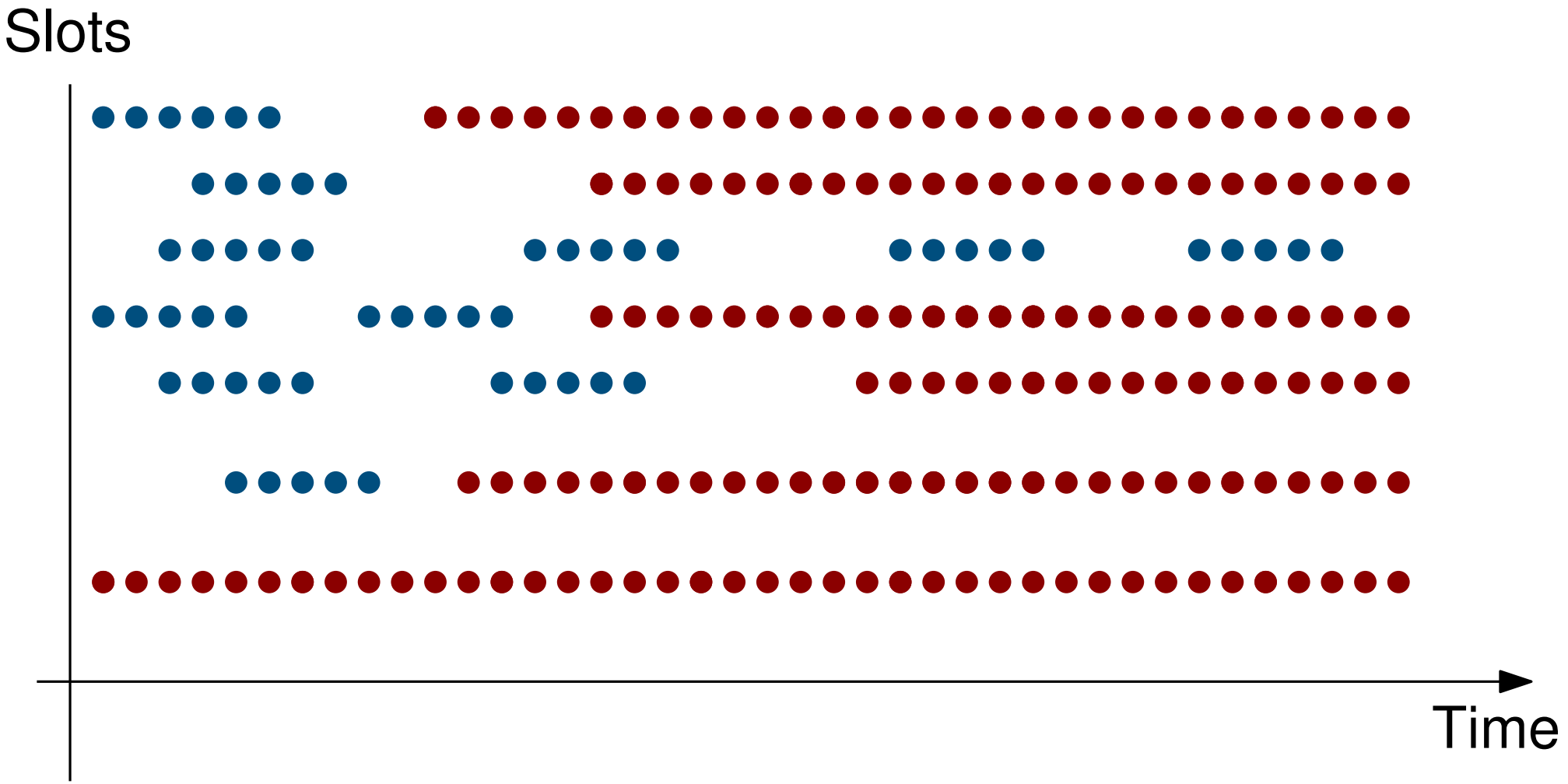
- Decide if the this new request is going to be processed;
- If so, then decide which one of the existing requests should be removed.

SeVen is a Selective Verification Tool.

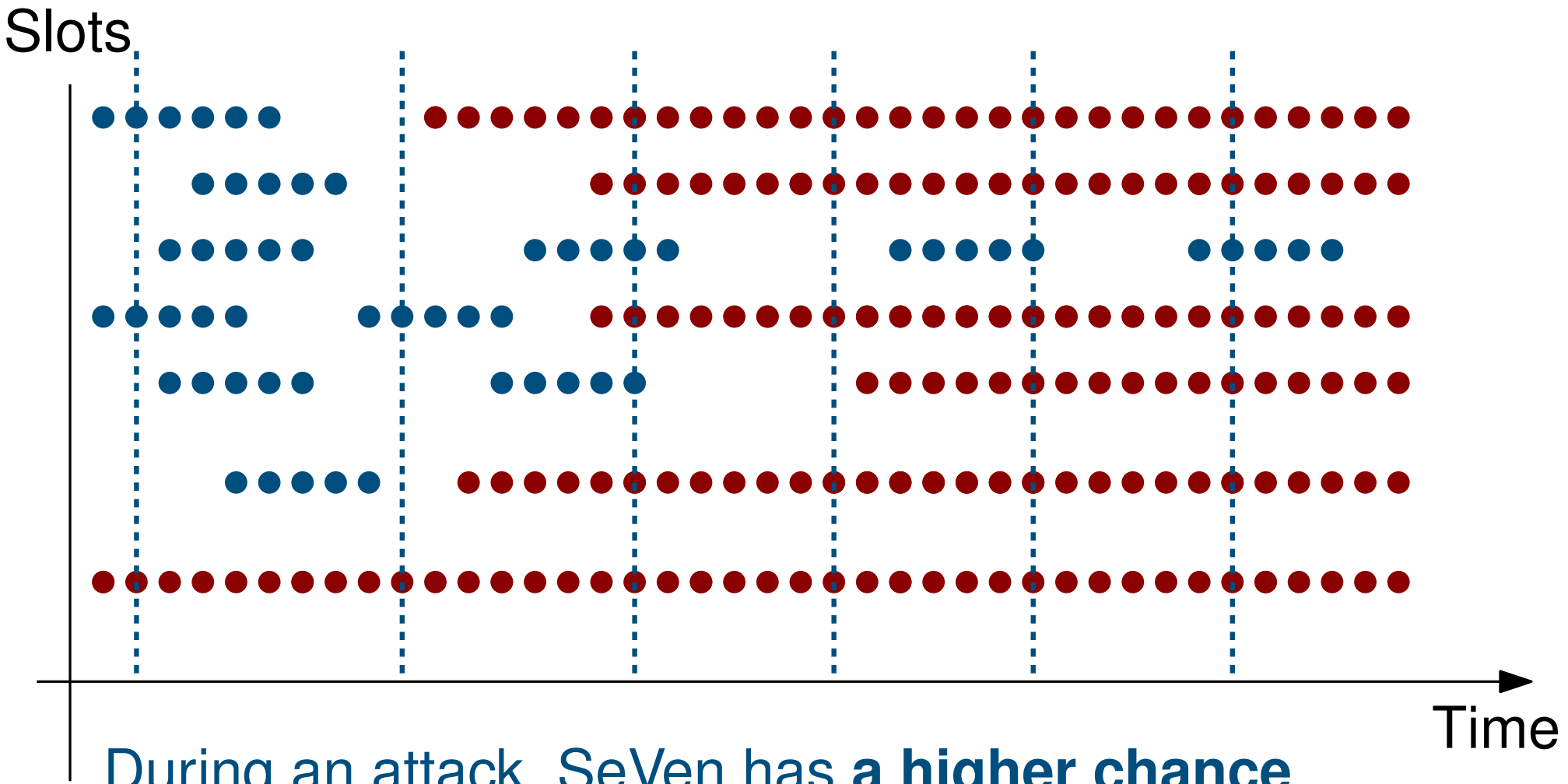
SeVen - Selective Verification Defense

- SeVen is agnostic with respect to the attack:
- When the web-server is overloaded SeVen **allows new request** to be processed.

Why does SeVen work?

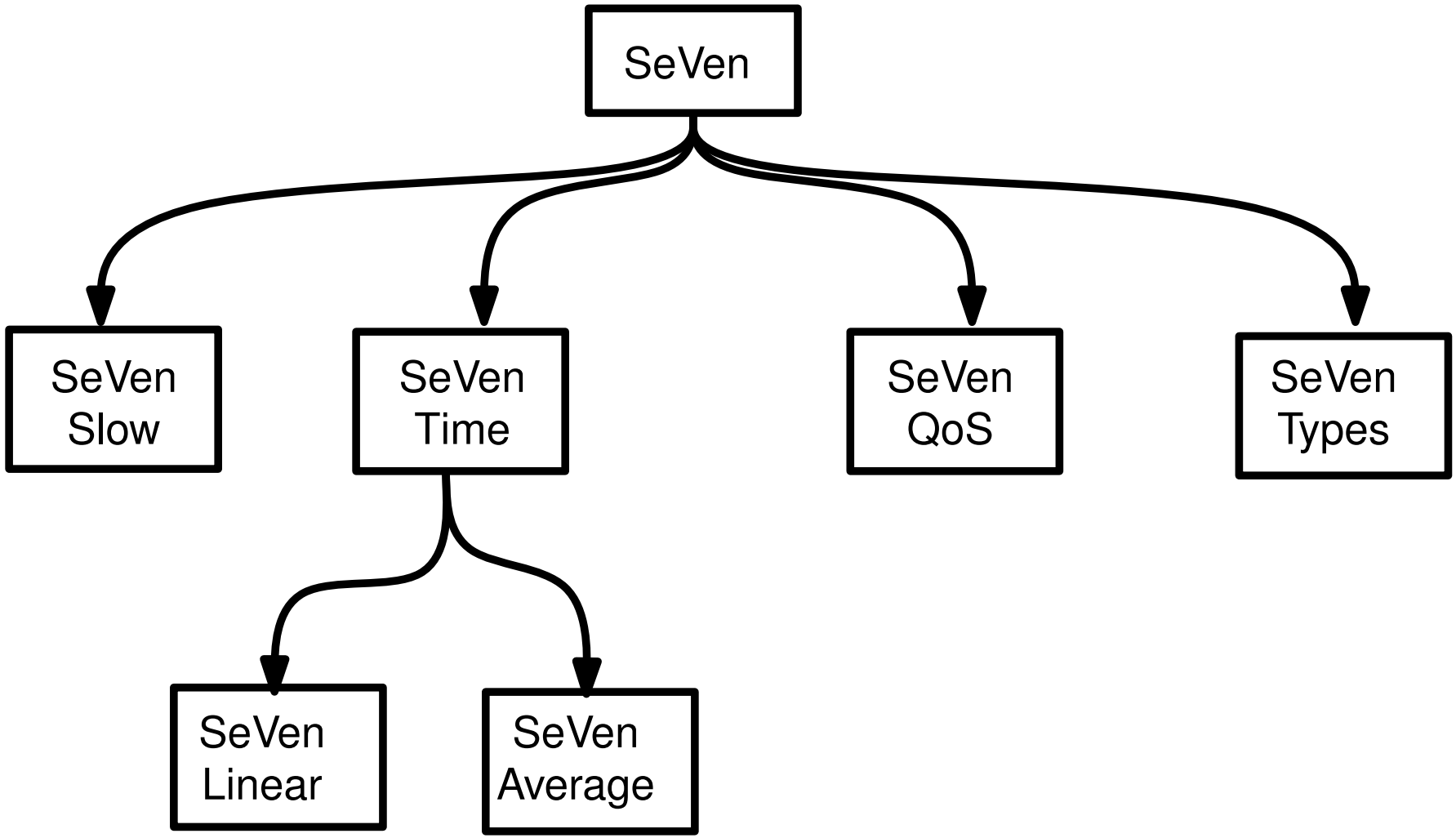


Why does SeVen work?

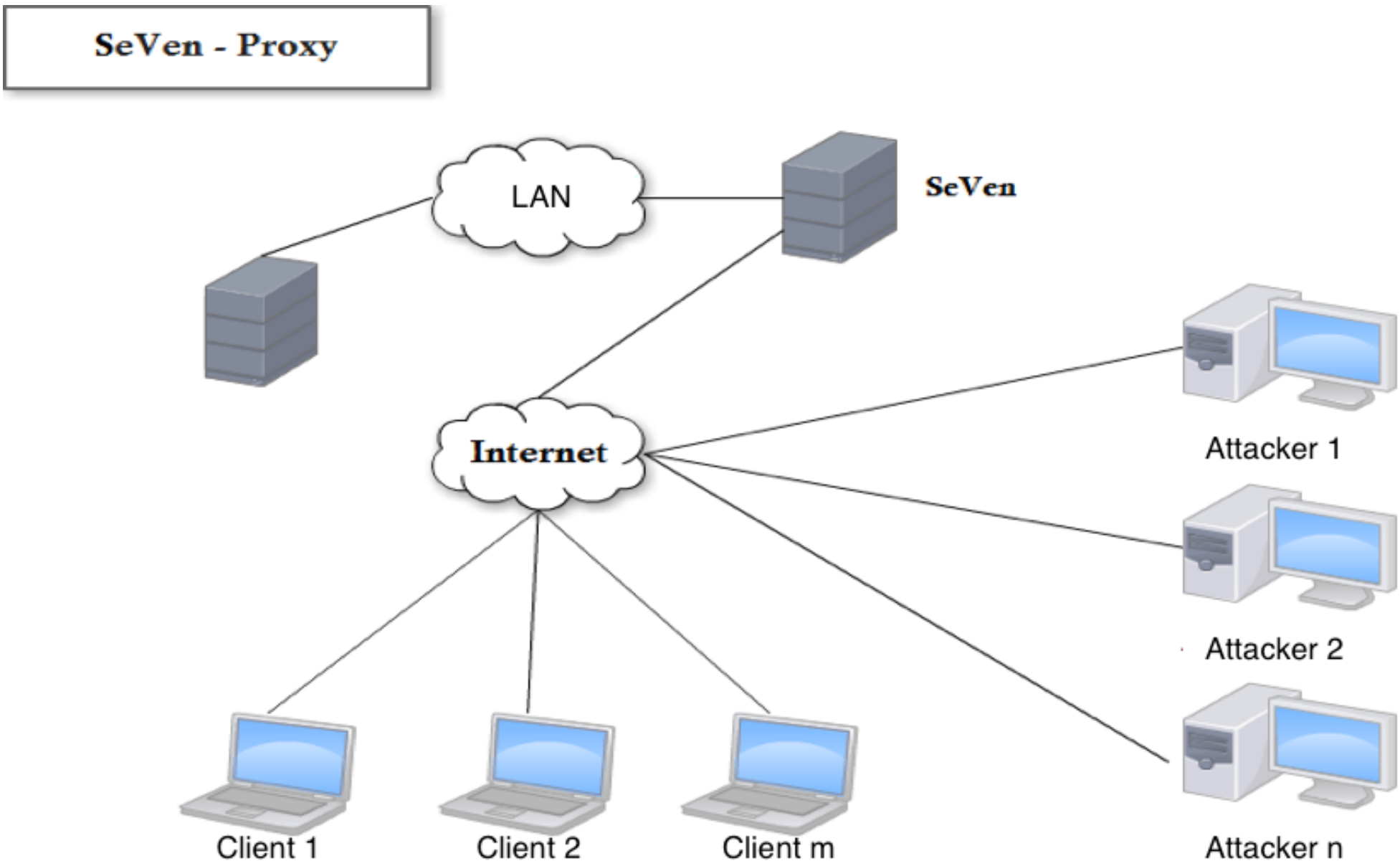


During an attack, SeVen has **a higher chance to drop an attacker than a legitimate client**.

Other instances of SeVen



Experimental Results



Experimental Results

- Carried out a **Slowloris attack** throughout the country.
- **No automatic defenses was able to detect our attack.**
- The attack could succesfully make the target web-server **unvailable to legitimate clients**.

Experimental Results

General Set-up

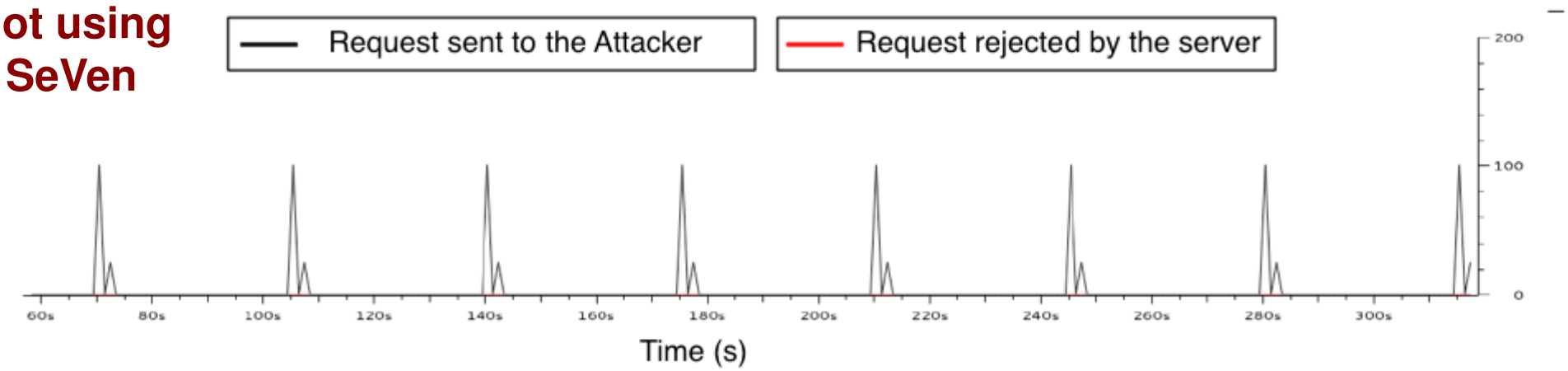
- **Apache 2.4**
  - Buffer: 200 positions
  - Timeout: 40s
- **SeVen**
  - Buffer: 200 positions
- **Time of Experiment**
  10 hours
- **Measurements**
  - Availability (Av)
  - Time to Service (TTS)

We used existing attacker tools and used Siege to emulate clients.

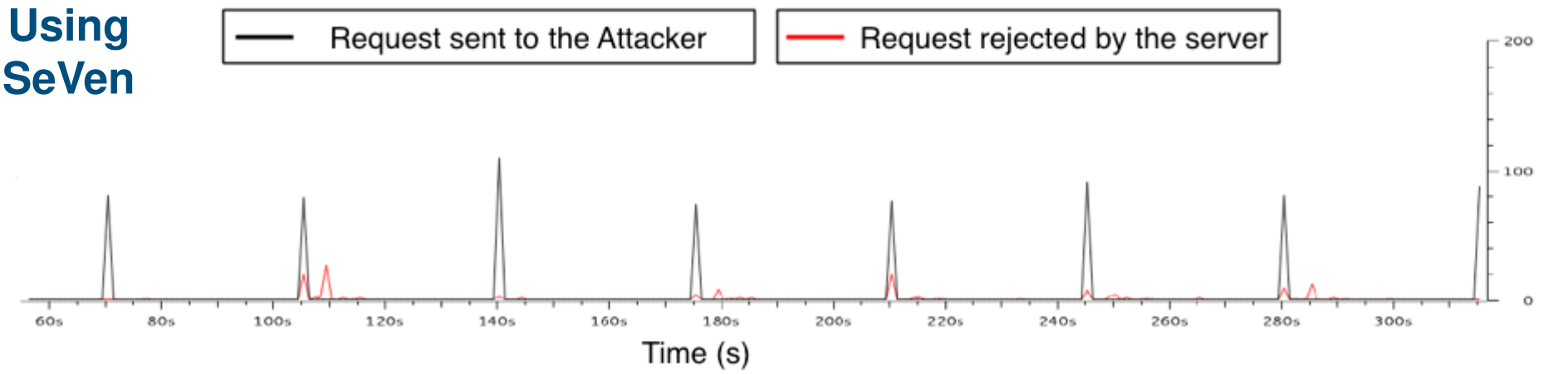
Experimental Results

Attacker Traffic – Slowloris Attack

Not using SeVen



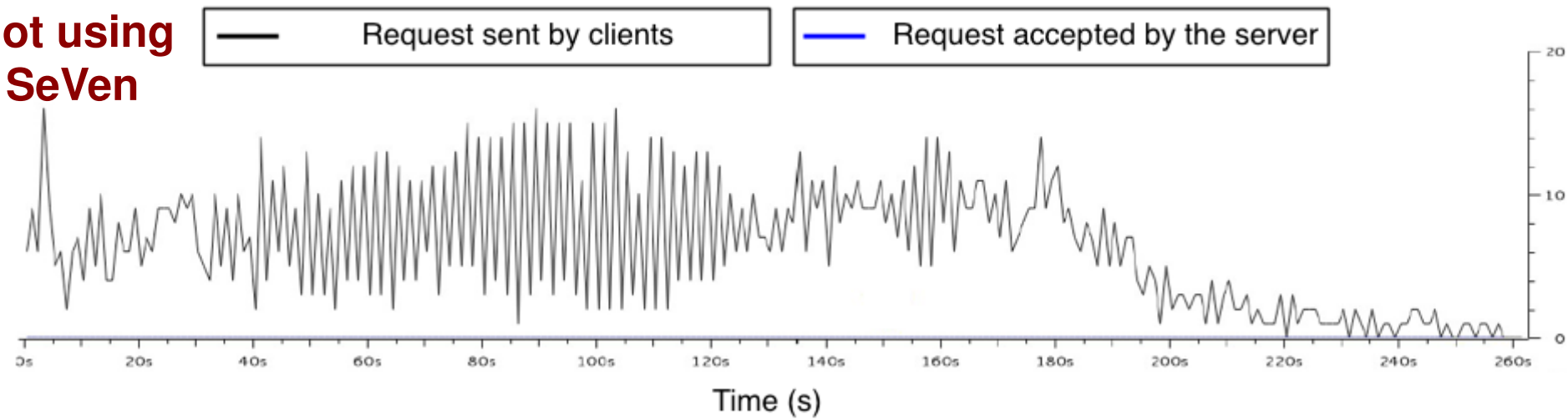
Using SeVen



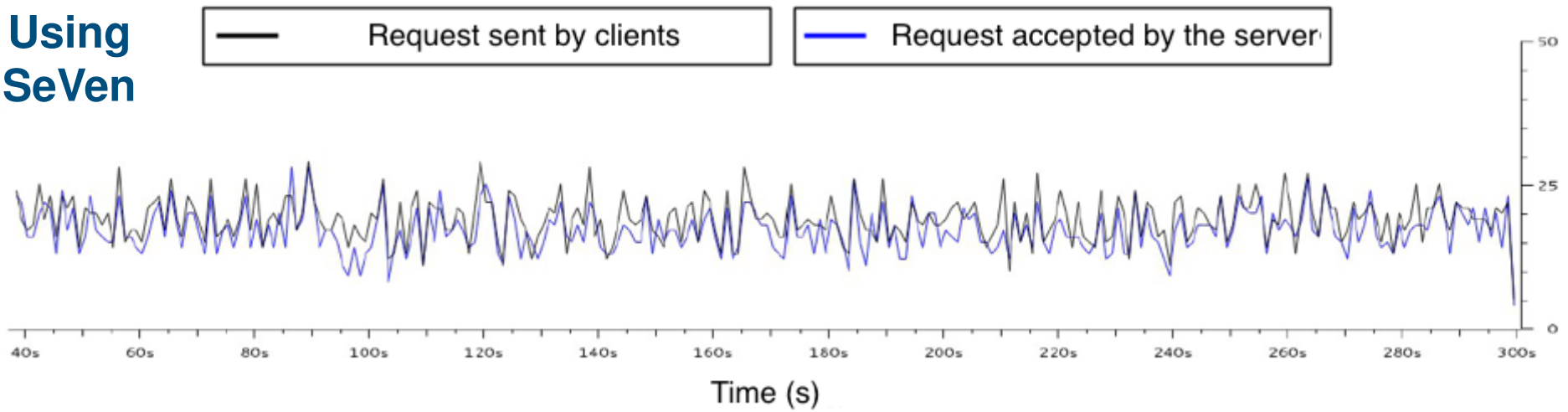
Experimental Results

Client Traffic – Slowloris Attack

Not using SeVen



Using SeVen



Experimental Results

	Not using SeVen		Using SeVen	
	Availability	TTS	Availability	TTS
No Attack	100%	0.01s	100%	0.11s
Slowloris	0.0%	∞	98.85%	0.15s
POST	0.0%	∞	97.25%	0.05s

Experimental Results

Slowloris

No Attack		Under Attack	
Memory	CPU	Memory	CPU
0.5%	0.9%	1%	1%

Conclusions and Future Work

- SeVen is a generic strategy for mitigating a large number of Application-Layer DDoS attacks.
- Our experiments demonstrate that SeVen is effective requiring very little computation power.

Future Work

- We are understanding better the impacts of SeVen on QoS.
- We are continuing to improve our implementations and testing its reliability.
- We are considering the use of SeVen in Application Layer DDoS exploiting other services, such as VoIP.

Questions?