

What is Distributed Denial of Service (DDoS)?

Gregory Travis

First, what is a Denial of

A denial of service is the deliberate or unintentional withholding of an expected service, utility,

- Examples:
 - Traffic jam caused by automotive accident
the utility of a highway

Denial of service

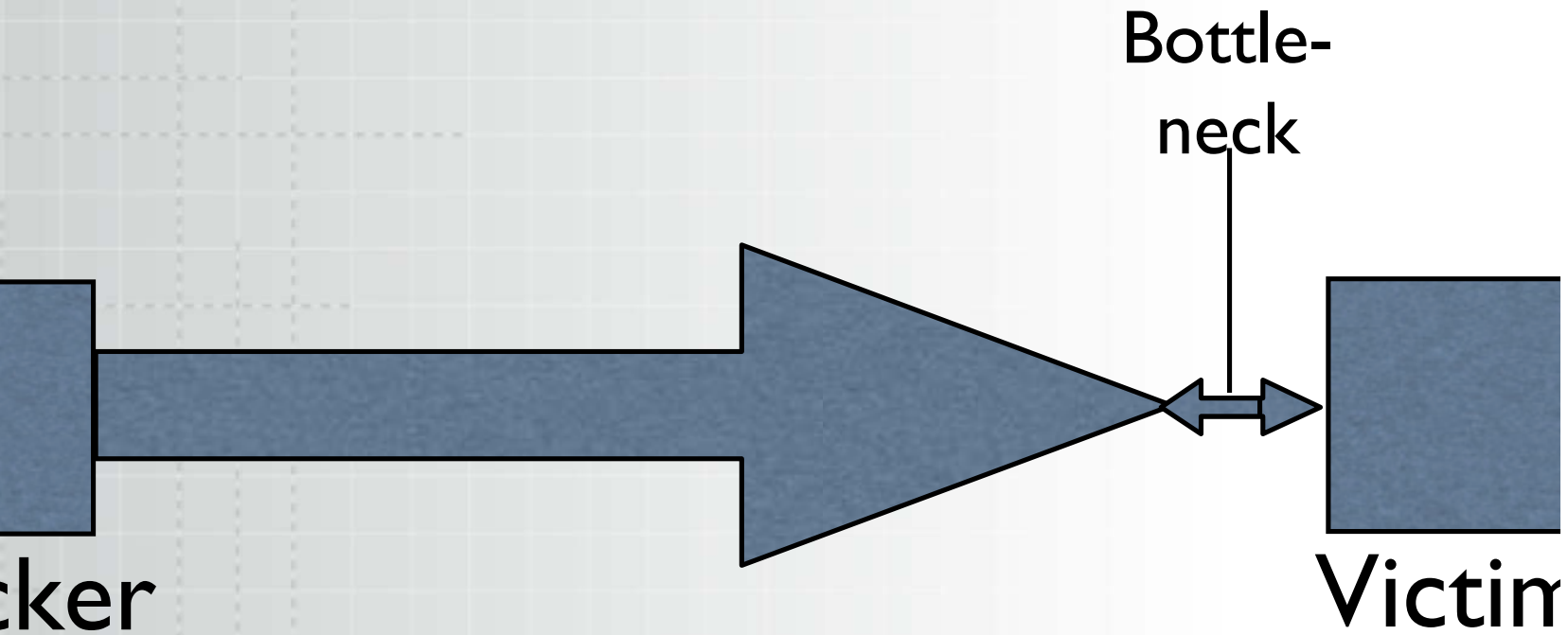
Although denials of service can be applied in ordinary situations, we are concerned exclusively with denials of service that occur within data network end systems (clients and servers)

Types of computerized service

Network denials:

- Simply flooding a network with enough traffic in an effort to deny the use of the network to its users (traffic-jam analogy)
- Attacking network infrastructure, such as routers and switches, in an effort to disable them

DoS Schematic - ban

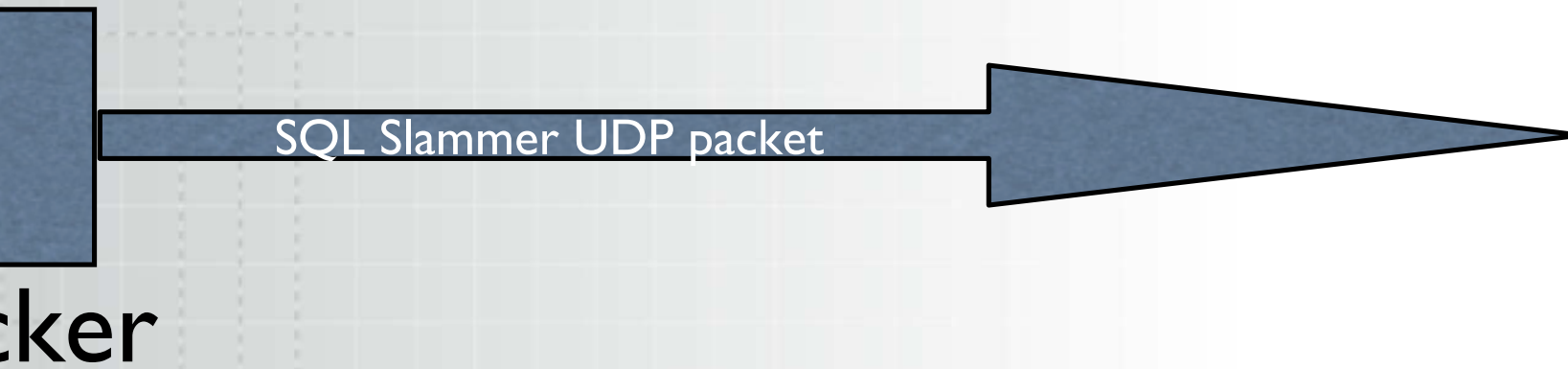


Types of computerized service

Server denials:

- Server or application crashes
 - The result of overload or known expl

DoS Schematic - e3



Distributed Denial of

Distributed Denial of Service is an enhanced standard denial of service techniques

- It utilizes several attackers instead of a single source hence the attack is “distributed”

Issues with distributed service

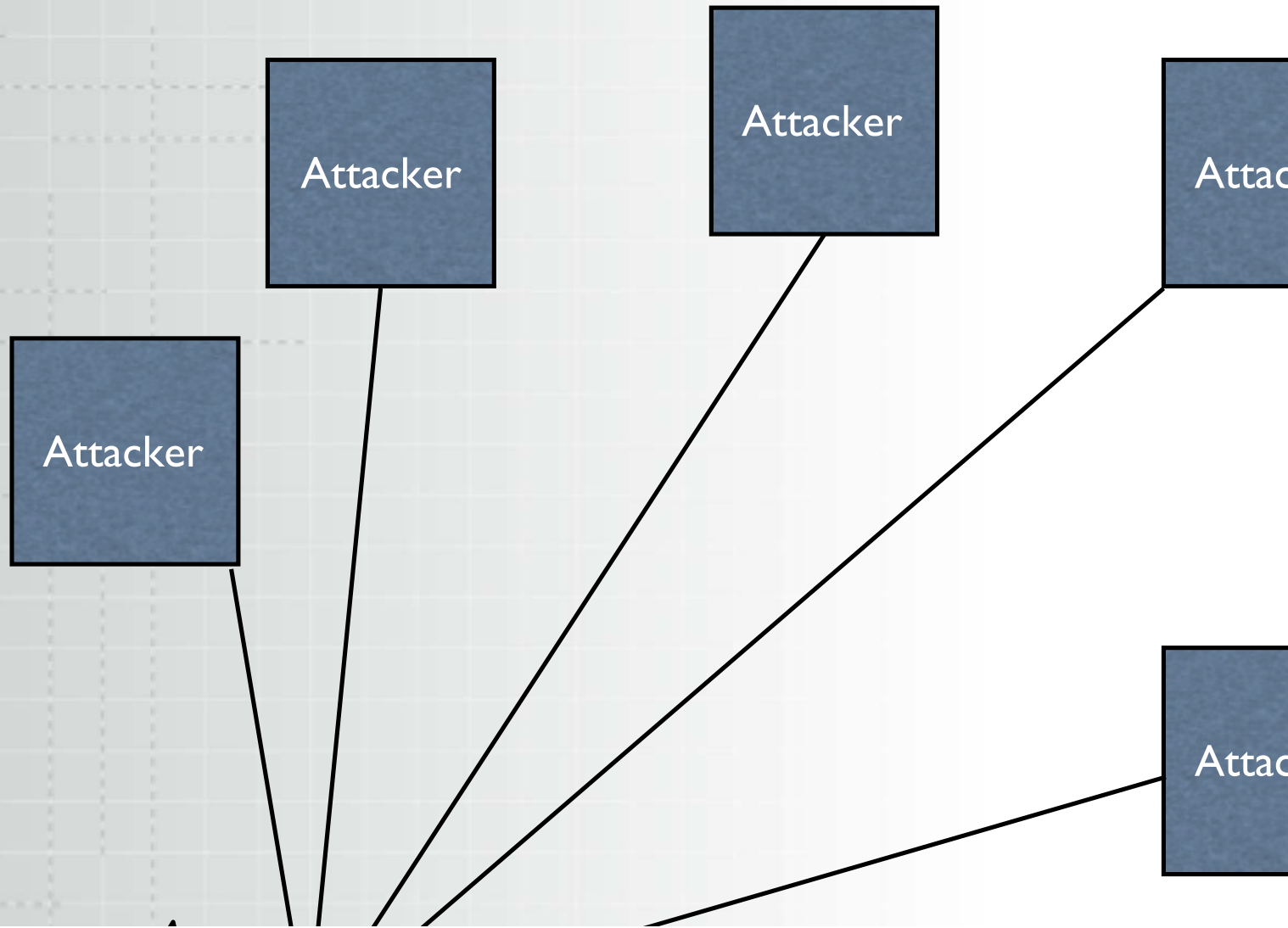
Distribution allows for aggregation of attac

- No one attacker needs to generate a sig
amount of data. Attack is aggregated at

Distribution makes it easier to conceal sou
attack

DDoS - Distributed

aggregation



How are systems comp

In classic DoS compromise of systems is not

- Example: Network flood from a single o system

DDoS comproi

DDoS usually involves compromising other systems

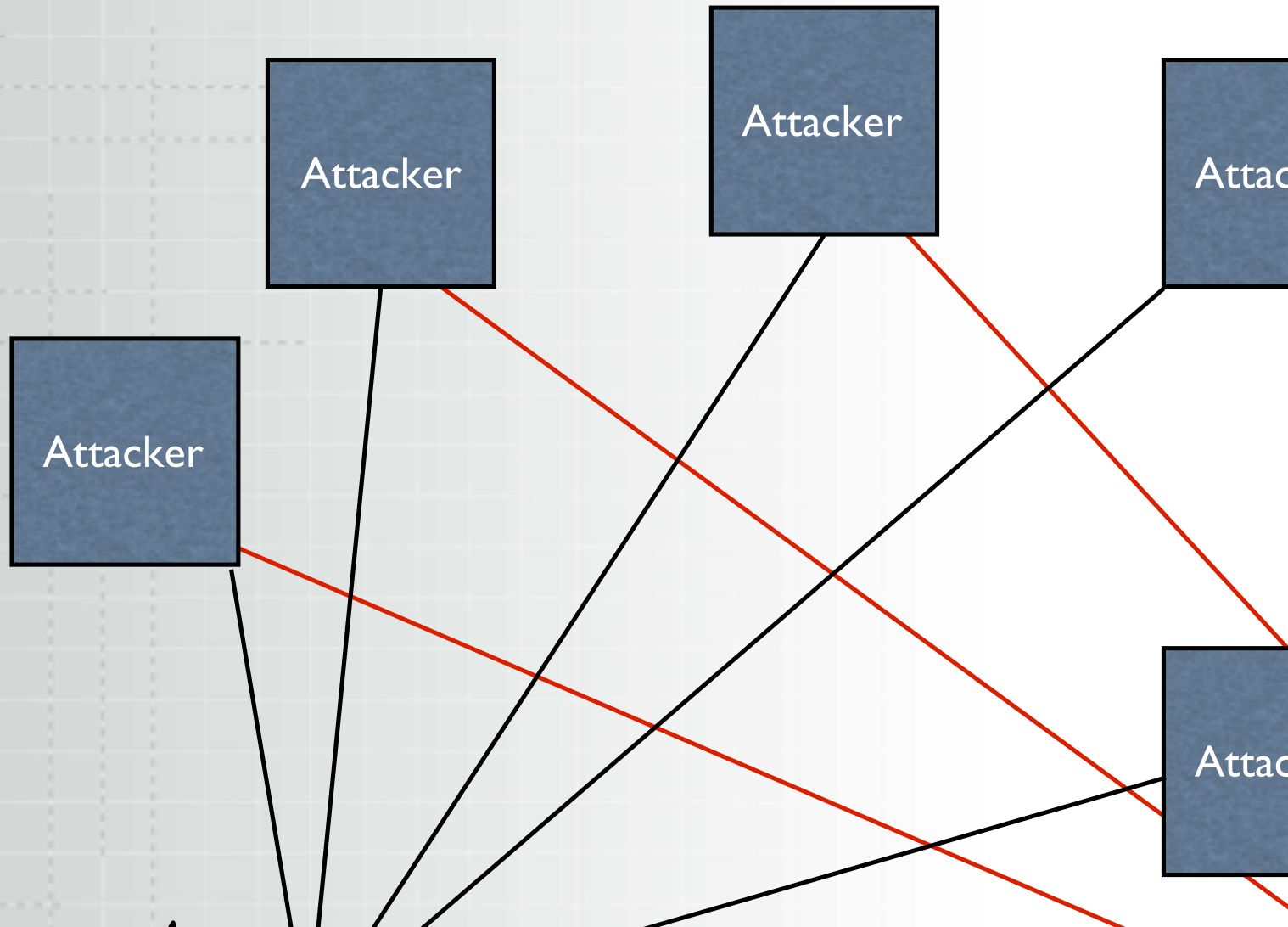
- Methods:
 - Mail/etc. macro viruses
 - Rootkits
 - Exploitation of known defects (i.e. buffer

DDoS Compro

Compromised (infected) systems begin DDoS in response to:

- Nothing, can initiate DDoS autonomous immediately (i.e. SQL Slammer)
- “Attack” signal from central “console”

DDoS - Distributed aggregation



Console/Attack commu

Typically the “console” communicates with attackers over a broadcast-type channel

- Important, for bad guy, that this commu concealed as it’s a way in which real bad conceal his/her location and identity
- To accomplish this they often use public (example AIM, IRC) and commands are

Timed attack rele

Next step was introduction of delay between
of commands and attack initiation

- Makes it much more difficult to connect
action

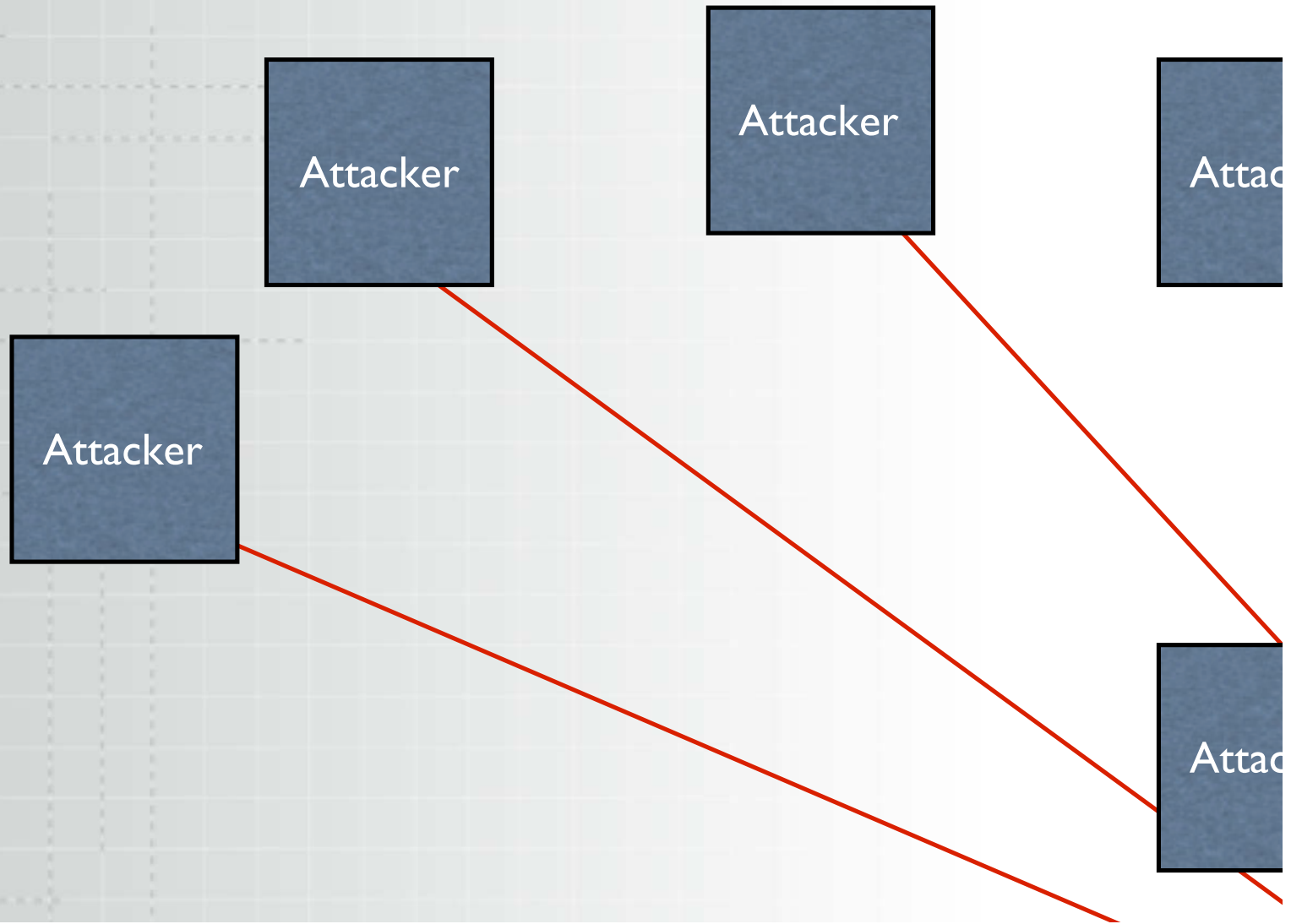
Pulsing Zomb

Final refinement was introduction of “pulsing

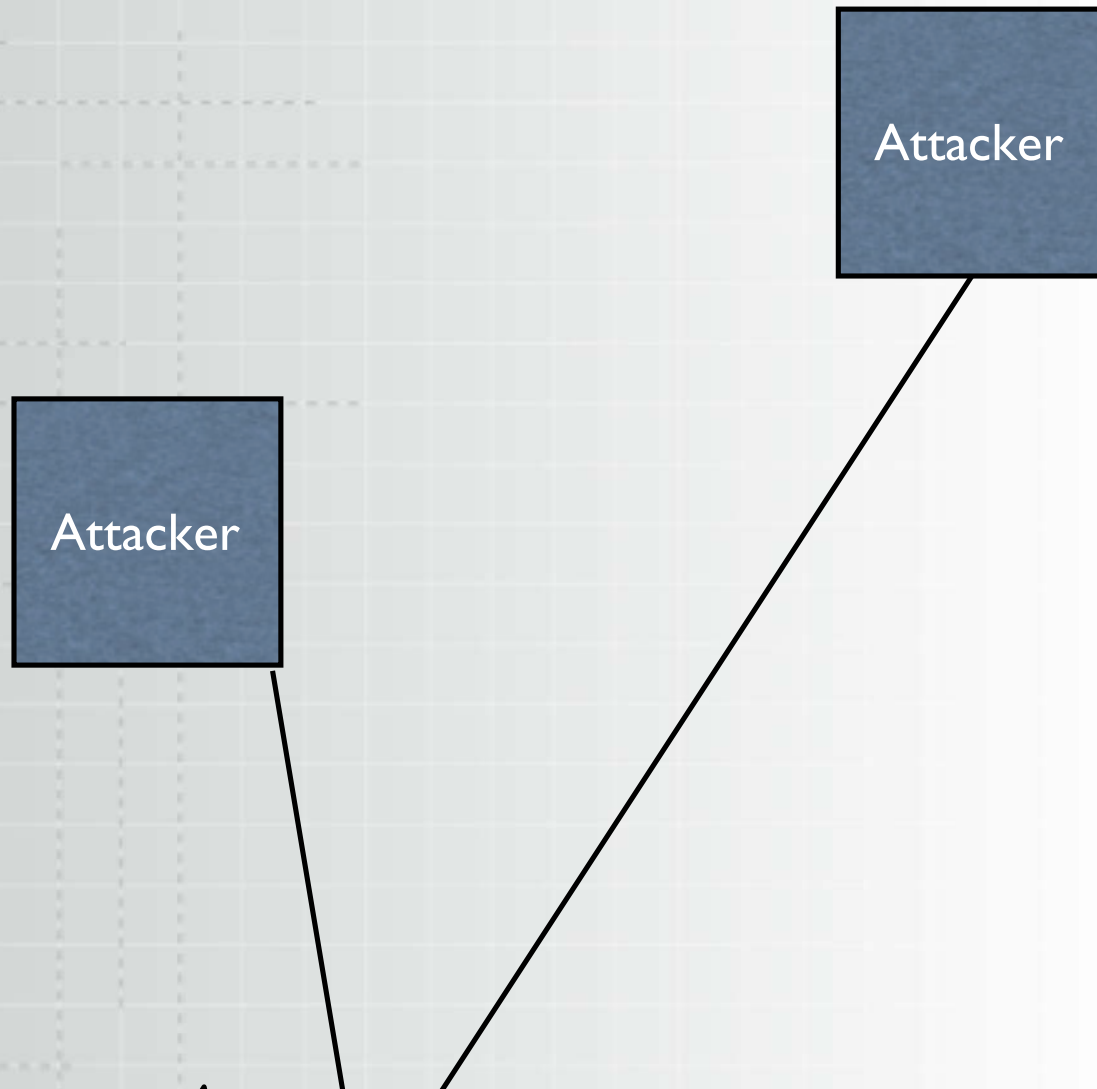
Like timed release but adds limit on length

- This way it's not only difficult to track by “console” but also to attackers as well. attacker only operates for a short time l dormant for a while. Difficult to trace

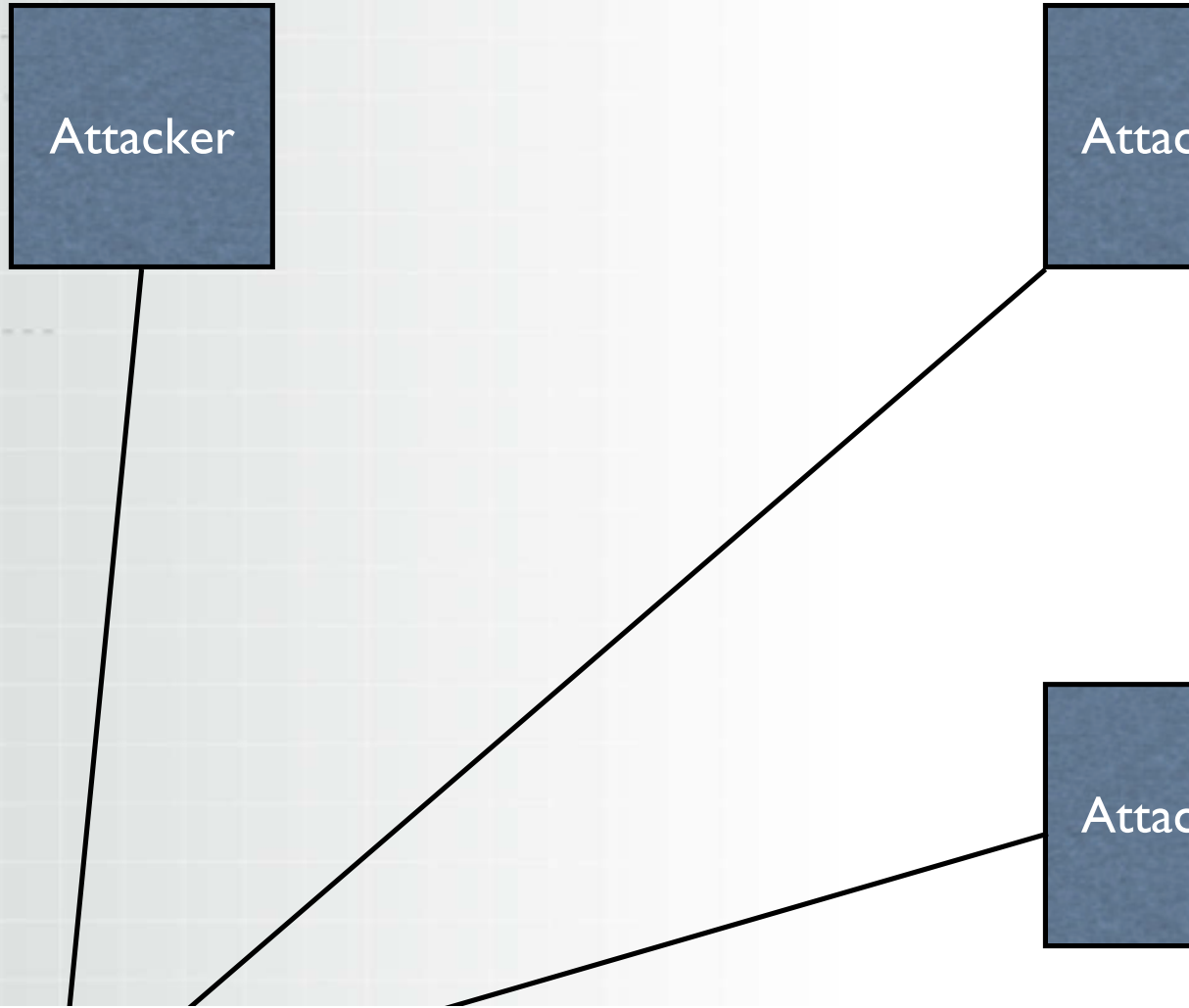
Zombie Setup



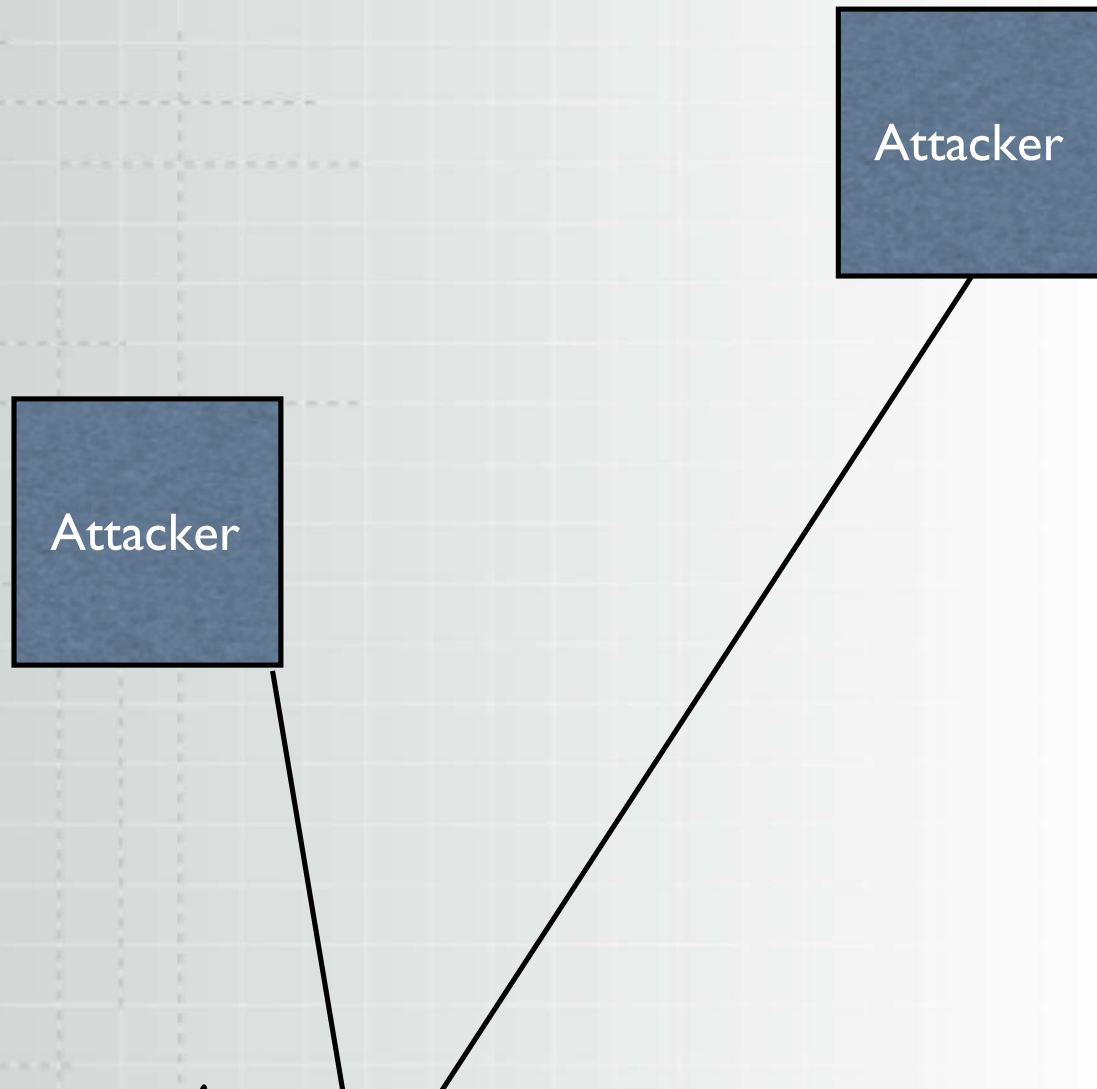
Zombie Attack



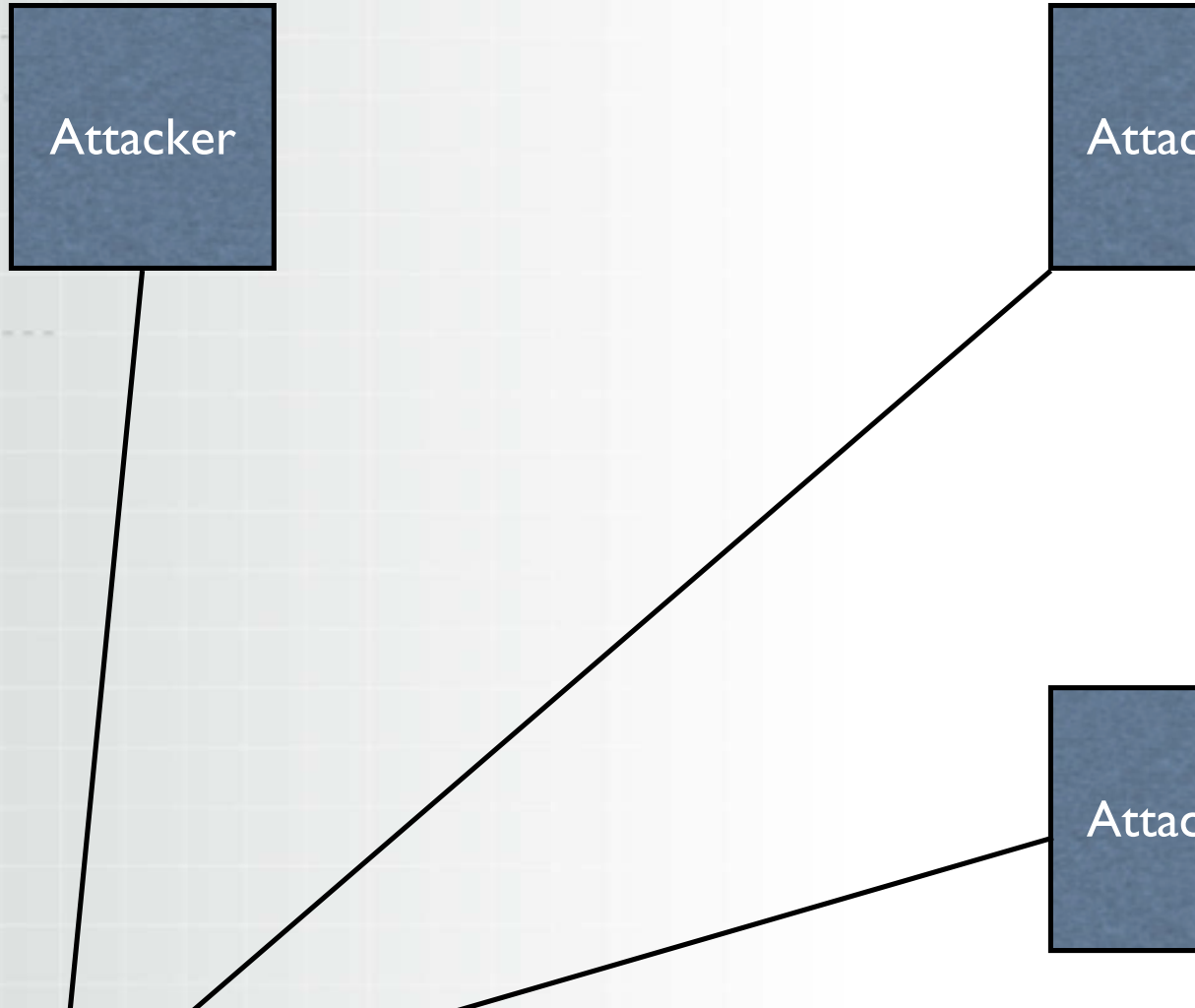
Zombie Attack



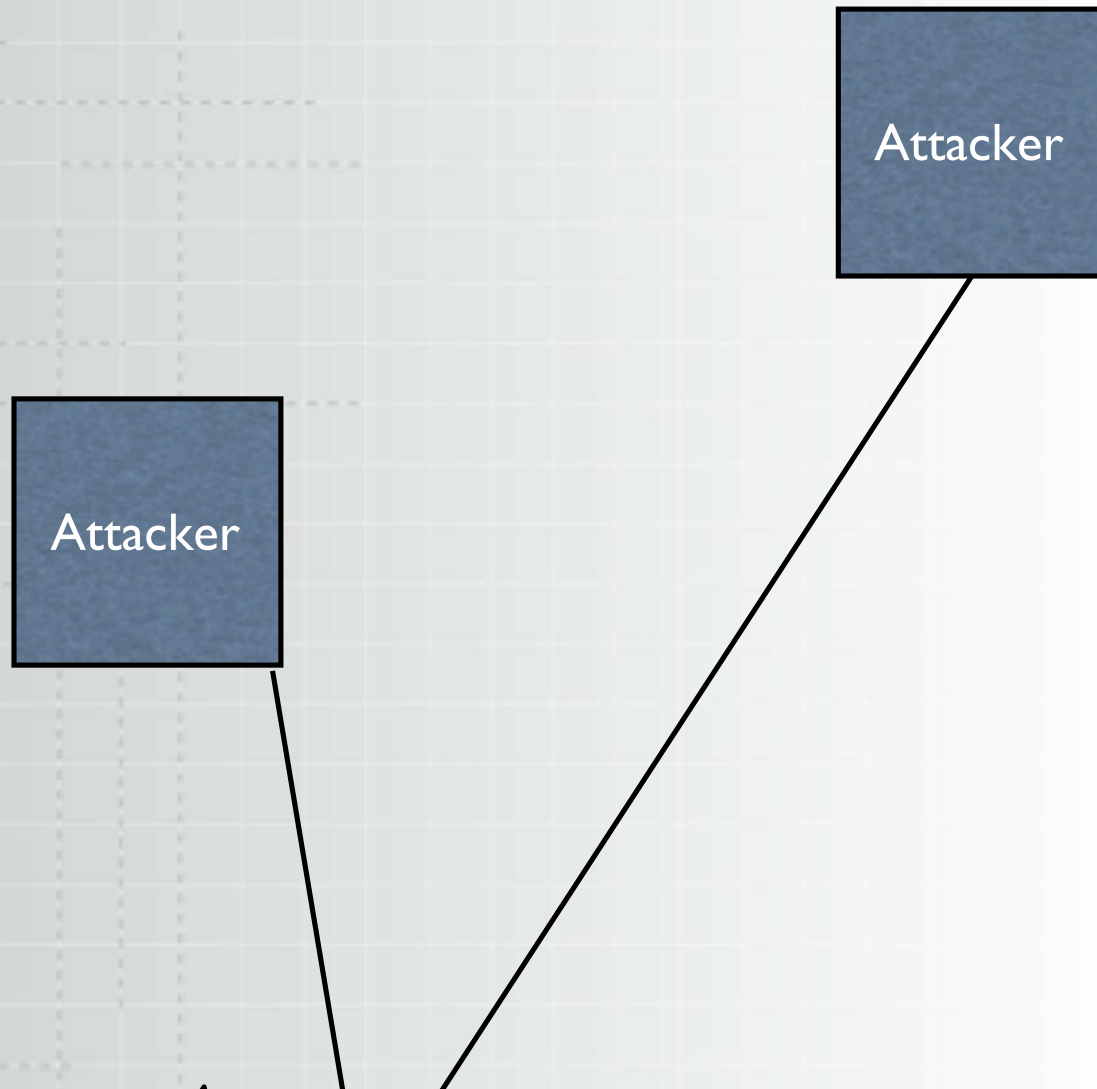
Zombie Attack



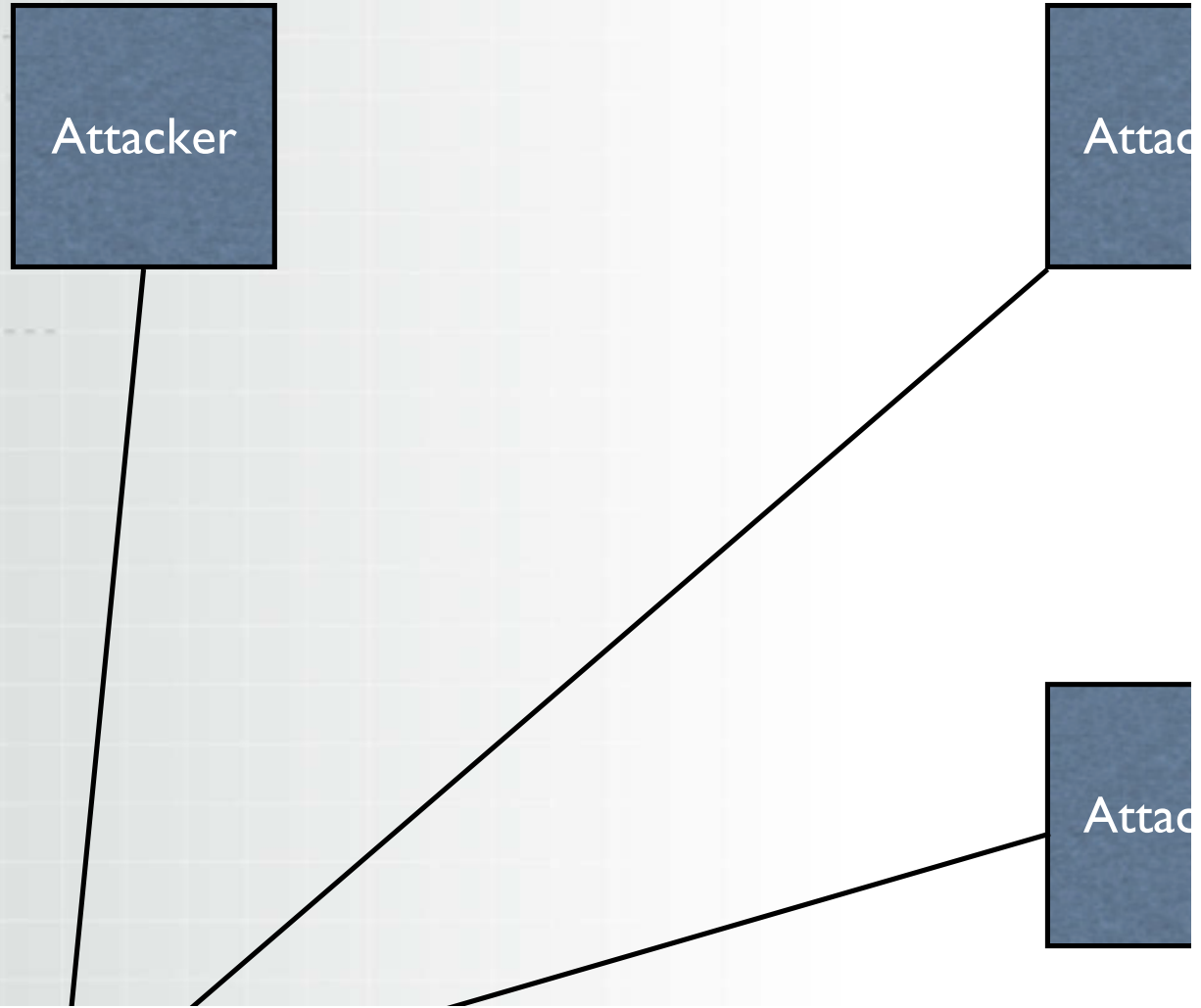
Zombie Attack



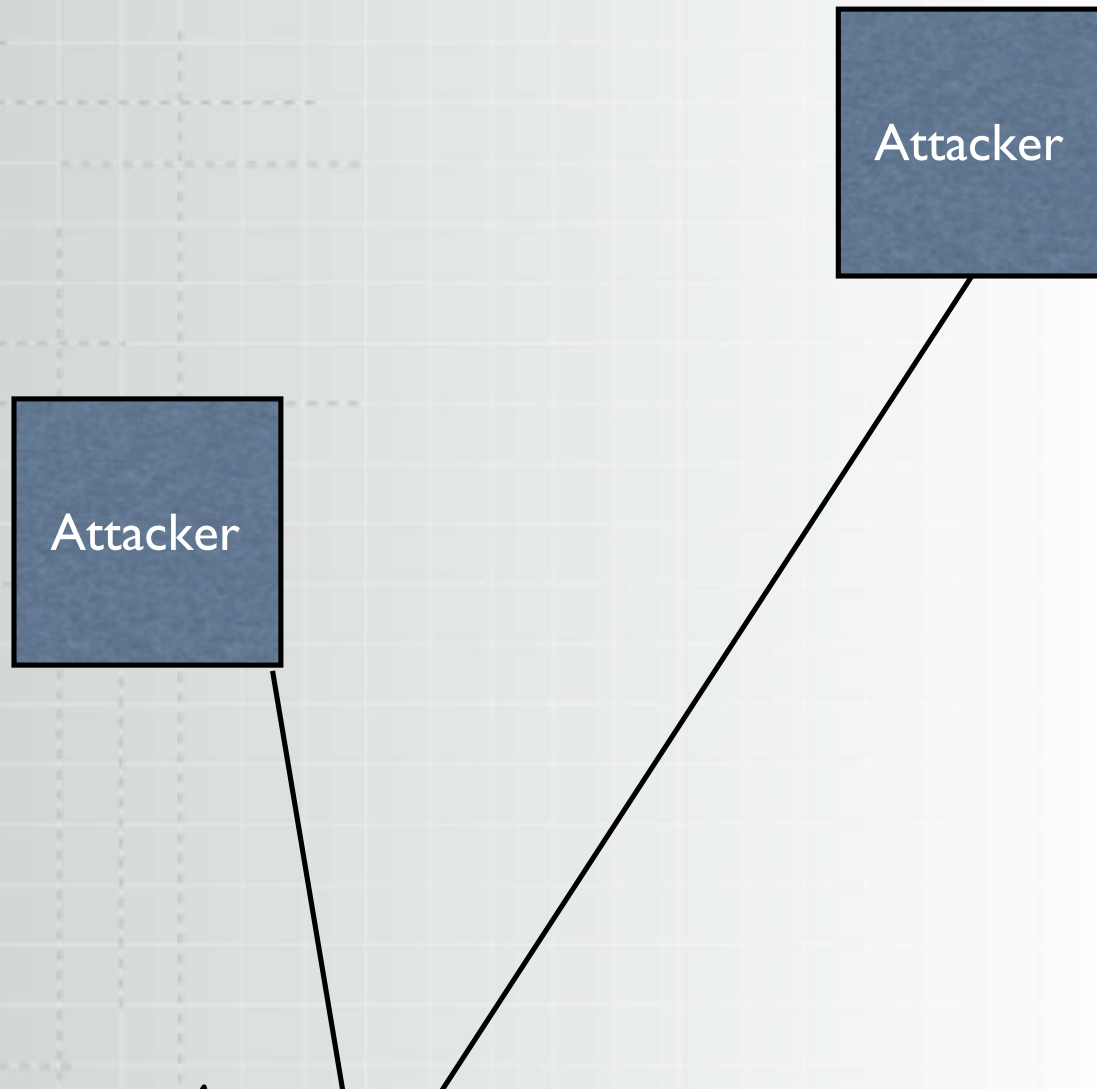
Zombie Attack



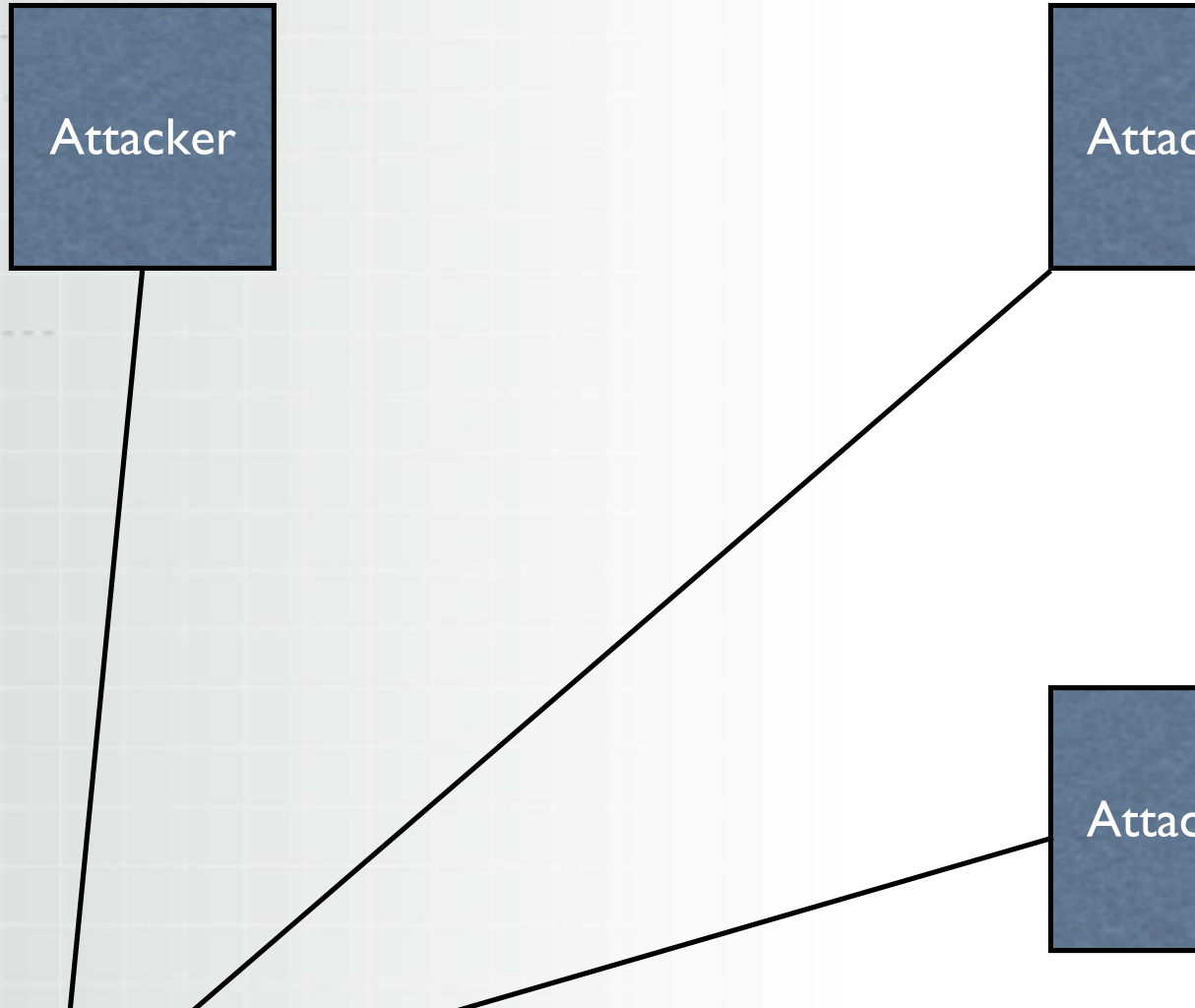
Zombie Attack



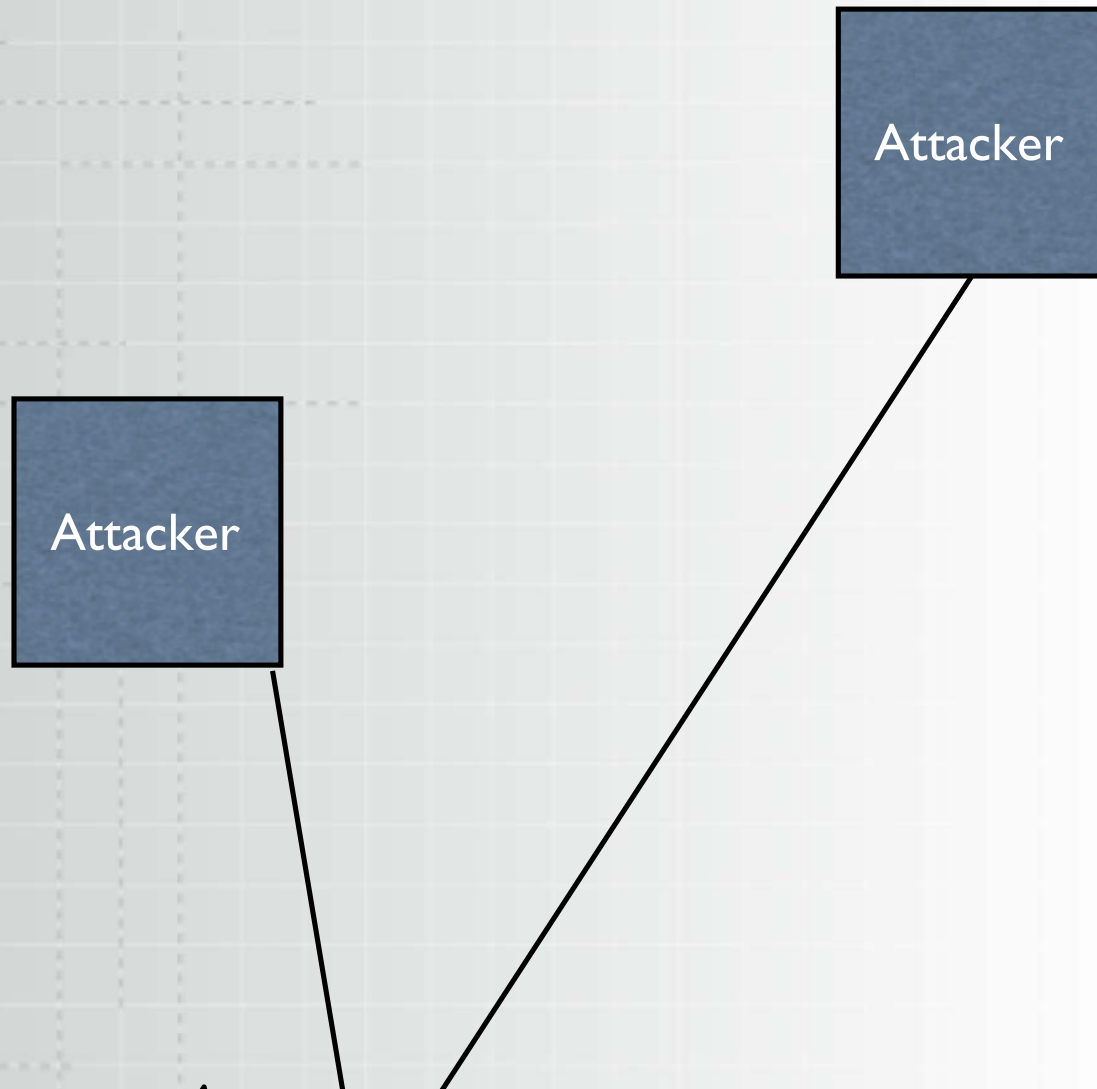
Zombie Attack



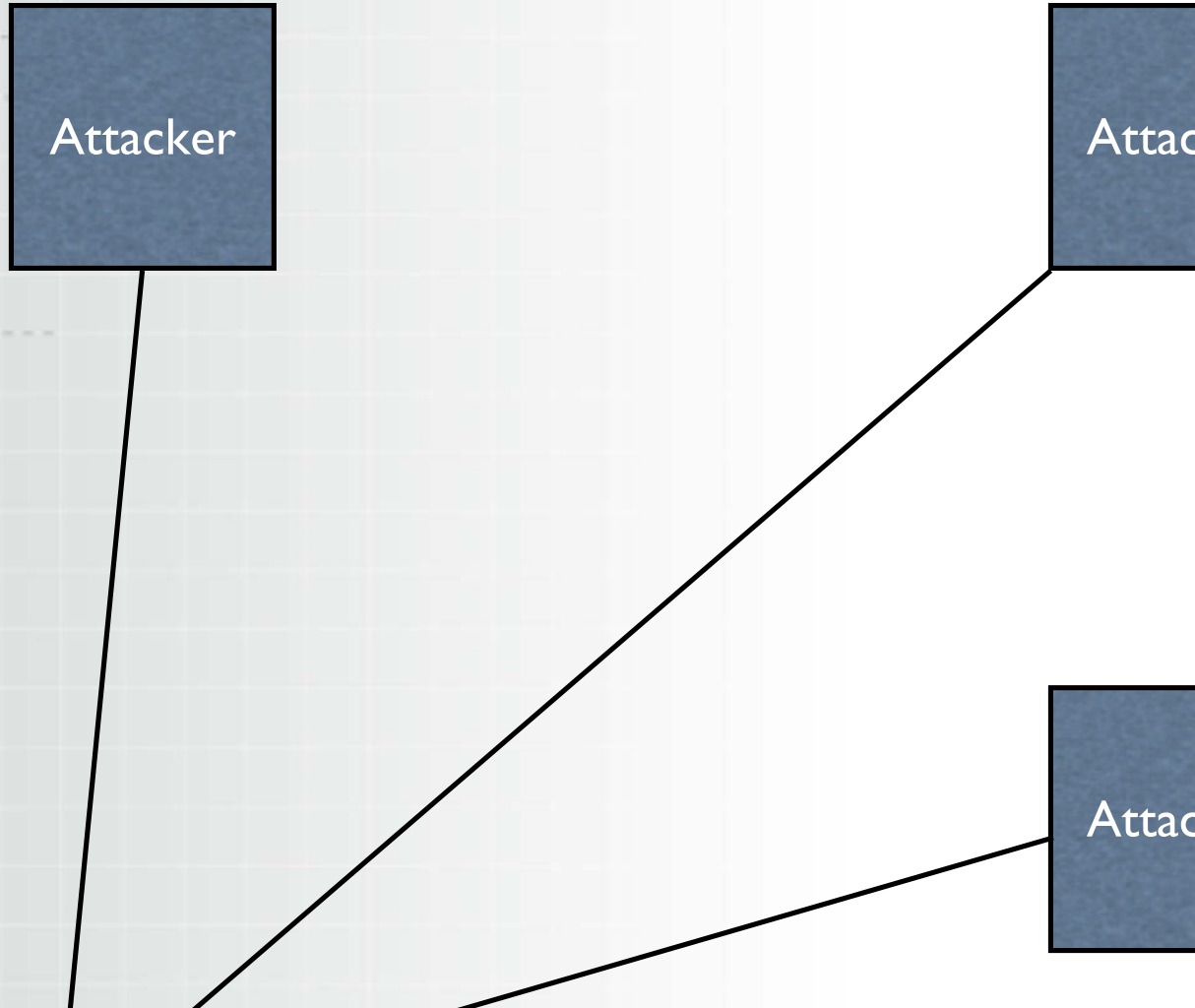
Zombie Attack



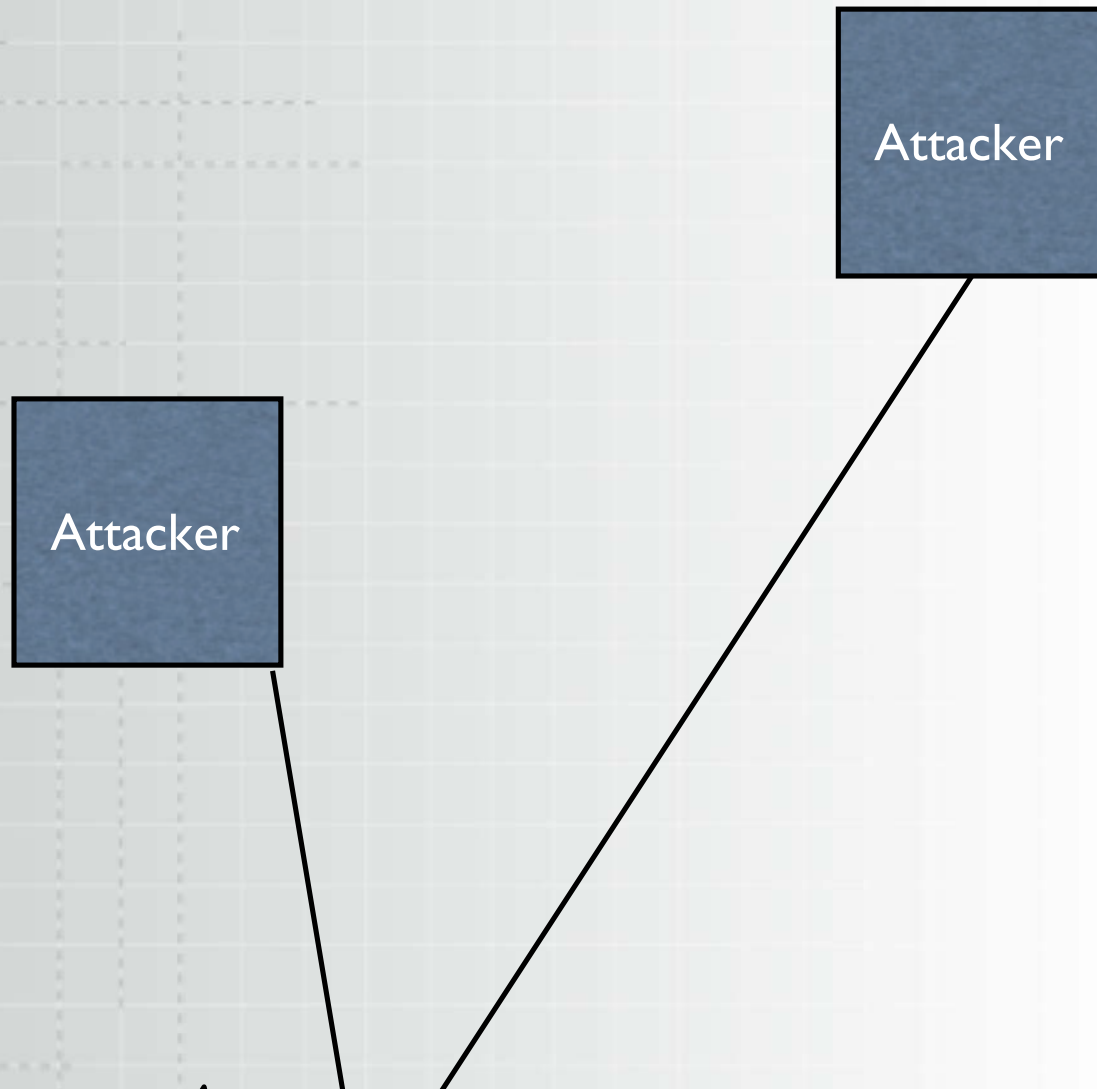
Zombie Attack



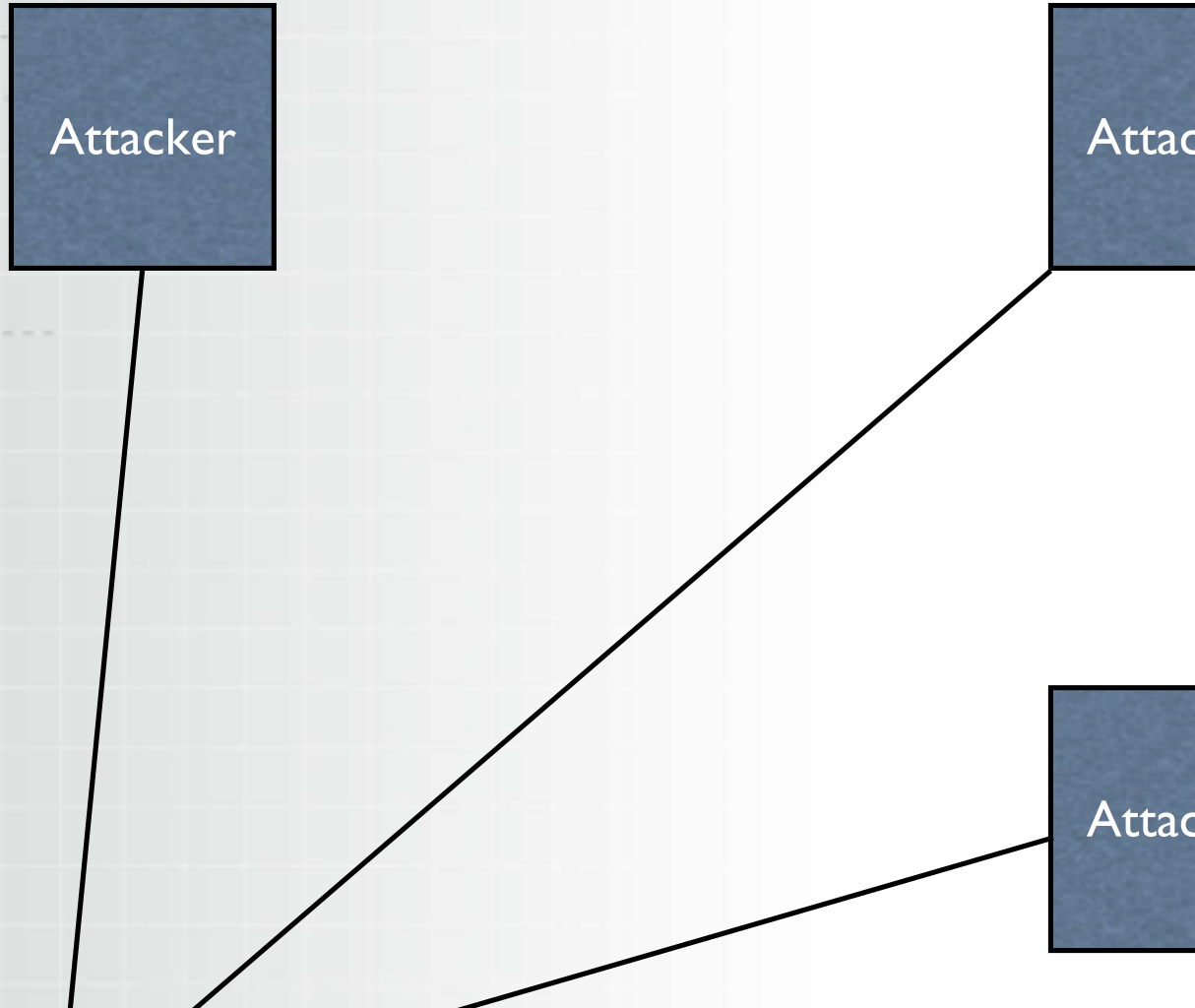
Zombie Attack



Zombie Attack



Zombie Attack



Wrapup

Evolution from DoS to DDoS to DDoS + ‘zombies’

Concept of a “console”

When compromise of systems is necessary
not