



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivet^{technology}labs.iu.edu

What is Distributed Denial of Service (DDoS)?

Gregory Travis
greg@iu.edu



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

First, what is a Denial of Service?

- A denial of service is the deliberate or unintentional withholding of an expected service, utility, or product.
- Examples:
 - Traffic jam caused by automotive accident denies the utility of a highway
 -



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Denial of service for us

- Although denials of service can be applied to many ordinary situations, we are concerned exclusively with denials of service that occur within data networks and at end systems (clients and servers)



Types of computerized denials of service

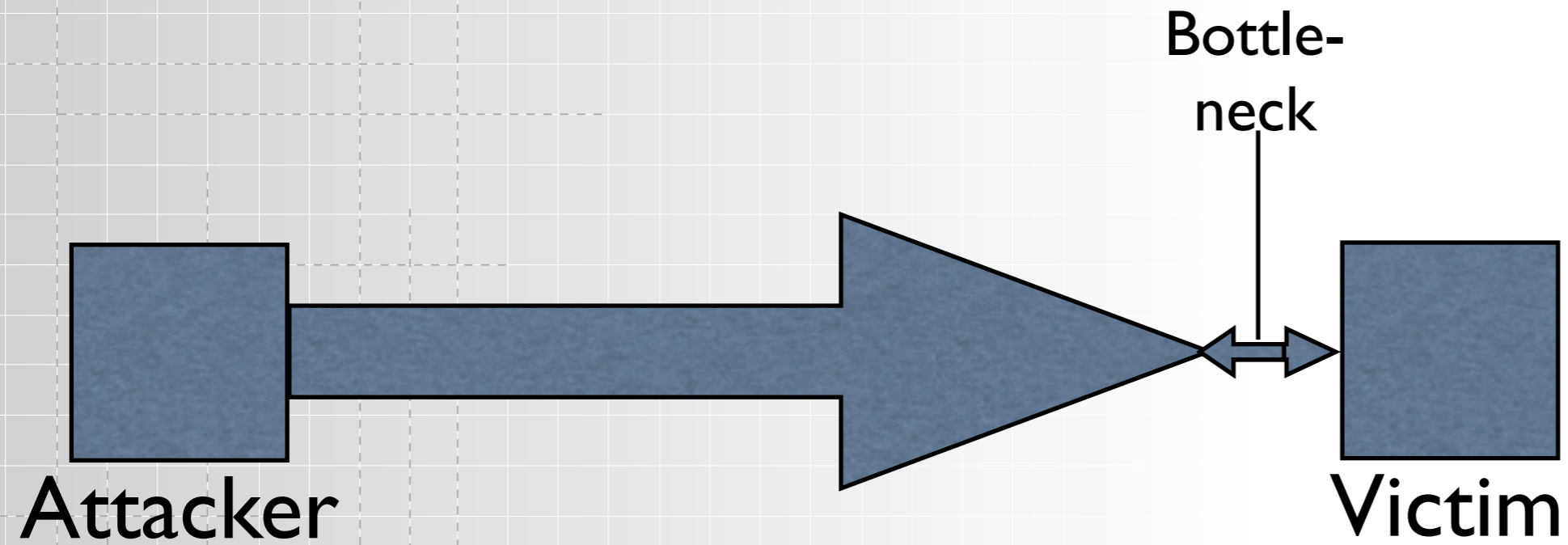
- Network denials:
 - Simply flooding a network with enough raw data in an effort to deny the use of the network by other users (traffic-jam analogy)
 - Attacking network infrastructure, such as routers, switches, etc. in an effort to disable them



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

DoS Schematic - bandwidth





pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

Types of computerized denials of service

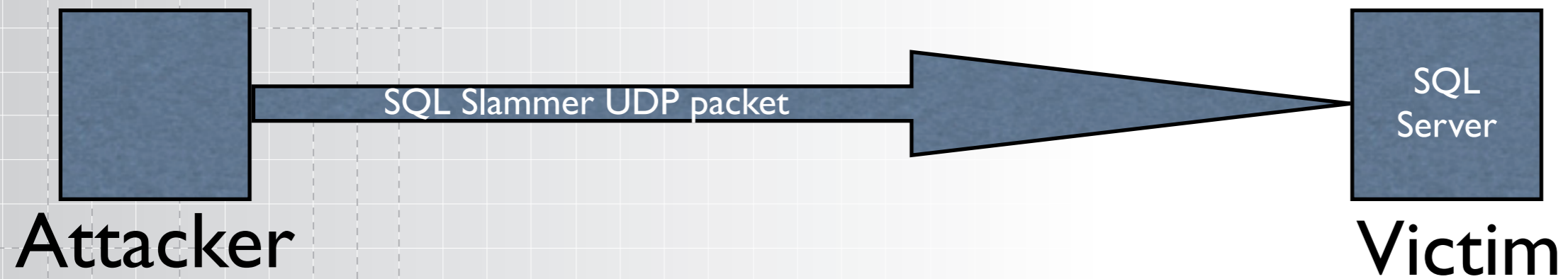
- Server denials:
 - Server or application crashes
 - The result of overload or known exploit



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

DoS Schematic - exploit





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Distributed Denial of Service

- Distributed Denial of Service is an enhancement to standard denial of service techniques
- It utilizes several attackers instead of a single one, hence the attack is “distributed”



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Issues with distributed denial of service

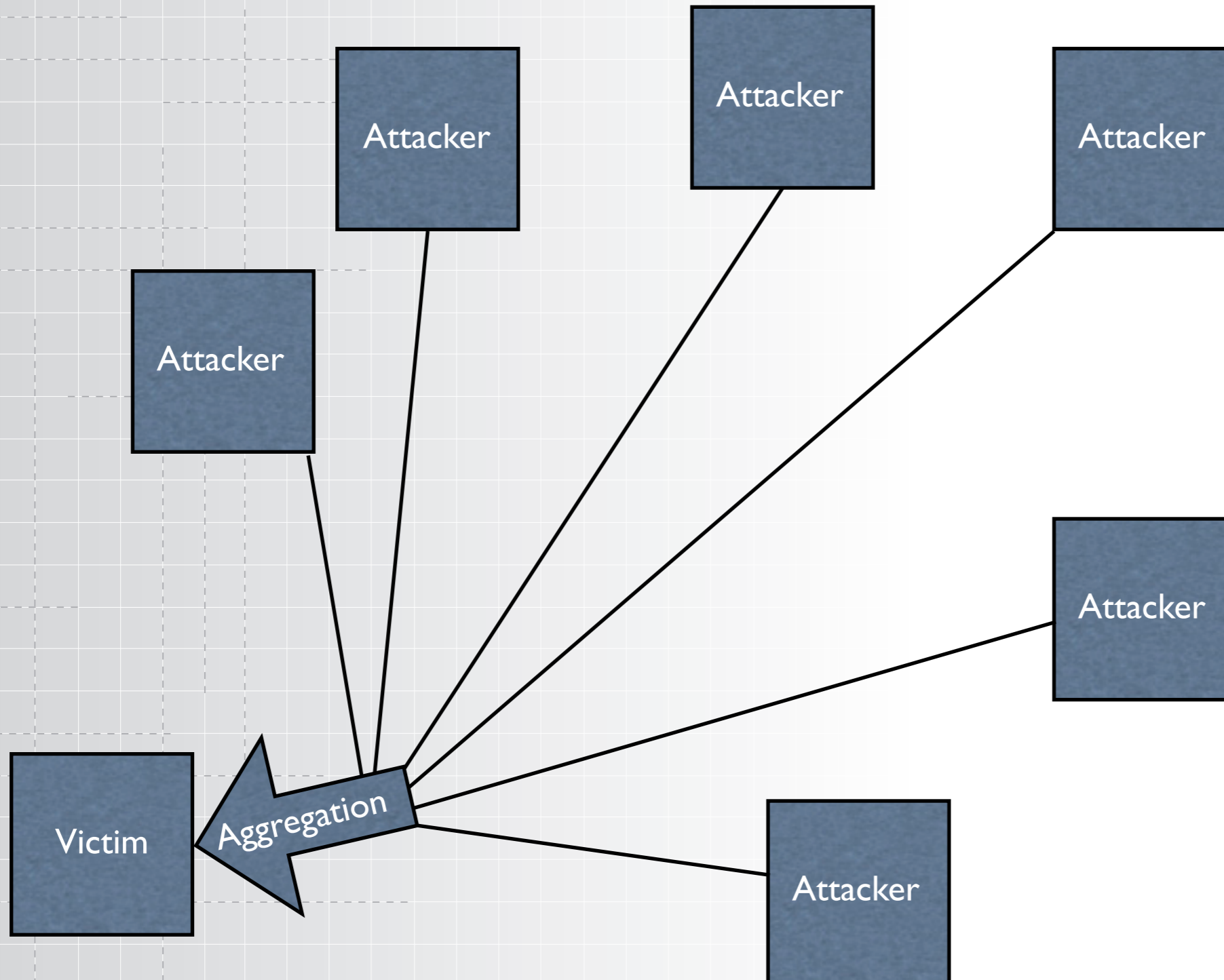
- Distribution allows for aggregation of attack
- No one attacker needs to generate a significant amount of data. Attack is aggregated at the receiver
- Distribution makes it easier to conceal source of attack



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

DDoS - Distribution and aggregation





pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivet^{technology}labs.iu.edu

How are systems compromised?

- In classic DoS compromise of systems is not necessary
 - Example: Network flood from a single owned system



DDoS compromise

- DDoS usually involves compromising other people's systems
- Methods:
 - Mail/etc. macro viruses
 - Rootkits
 - Exploitation of known defects (i.e. buffer overflow)

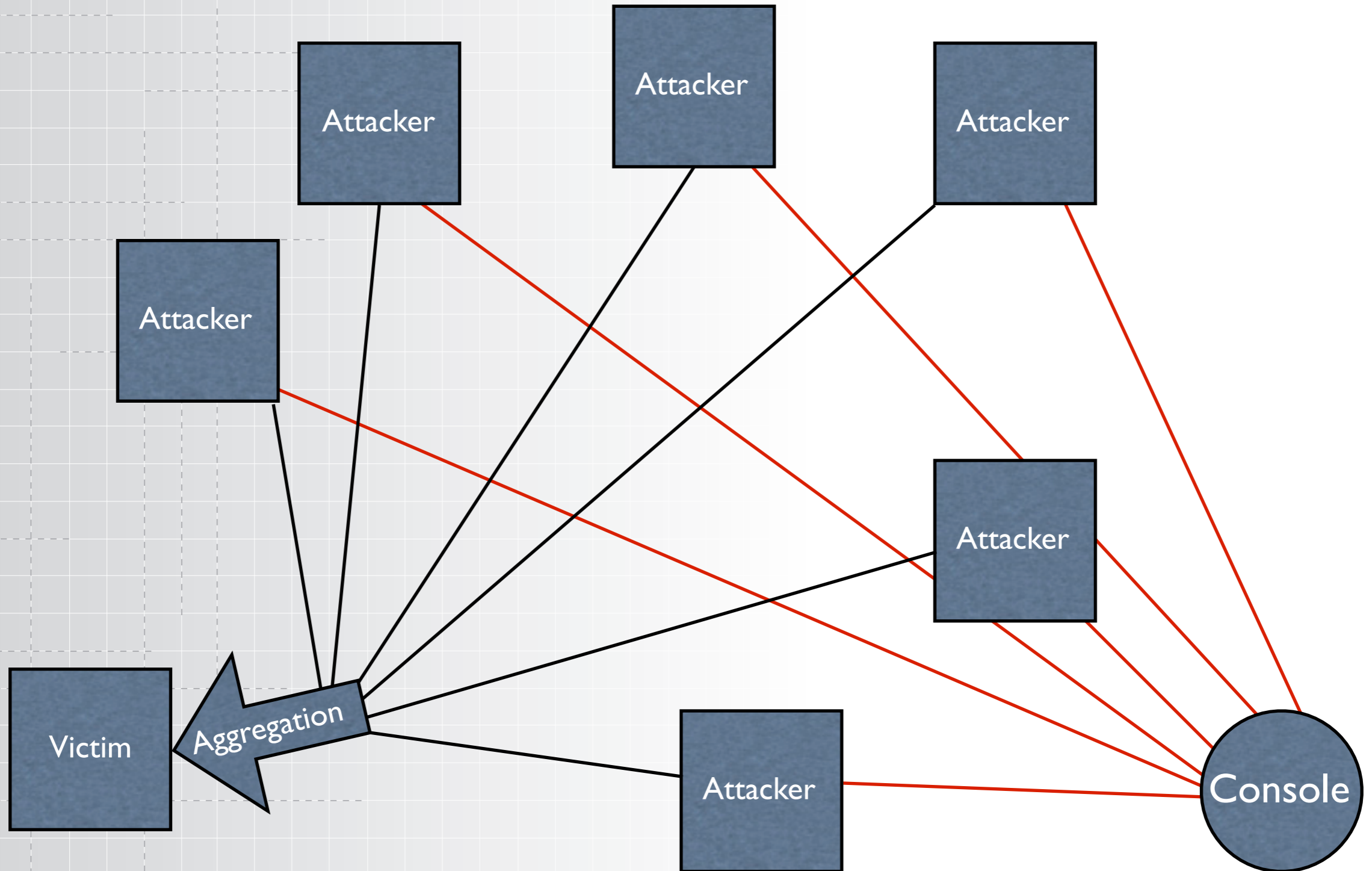


DDoS Compromise

- Compromised (infected) systems begin DDoS activity in response to:
 - Nothing, can initiate DDoS autonomously and immediately (i.e. SQL Slammer)
 - “Attack” signal from central “console”
 - Timer expiration



DDoS - Distribution and aggregation





Console/Attack communication

- Typically the “console” communicates with individual attackers over a broadcast-type channel
- Important, for bad guy, that this communication be concealed as it’s a way in which real bad guy can conceal his/her location and identity
- To accomplish this they often use public channels (example, AIM, IRC) and commands are disguised as ordinary “chatter.”



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Timed attack release

- Next step was introduction of delay between sending of commands and attack initiation
- Makes it much more difficult to connect console to action





Pulsing Zombies

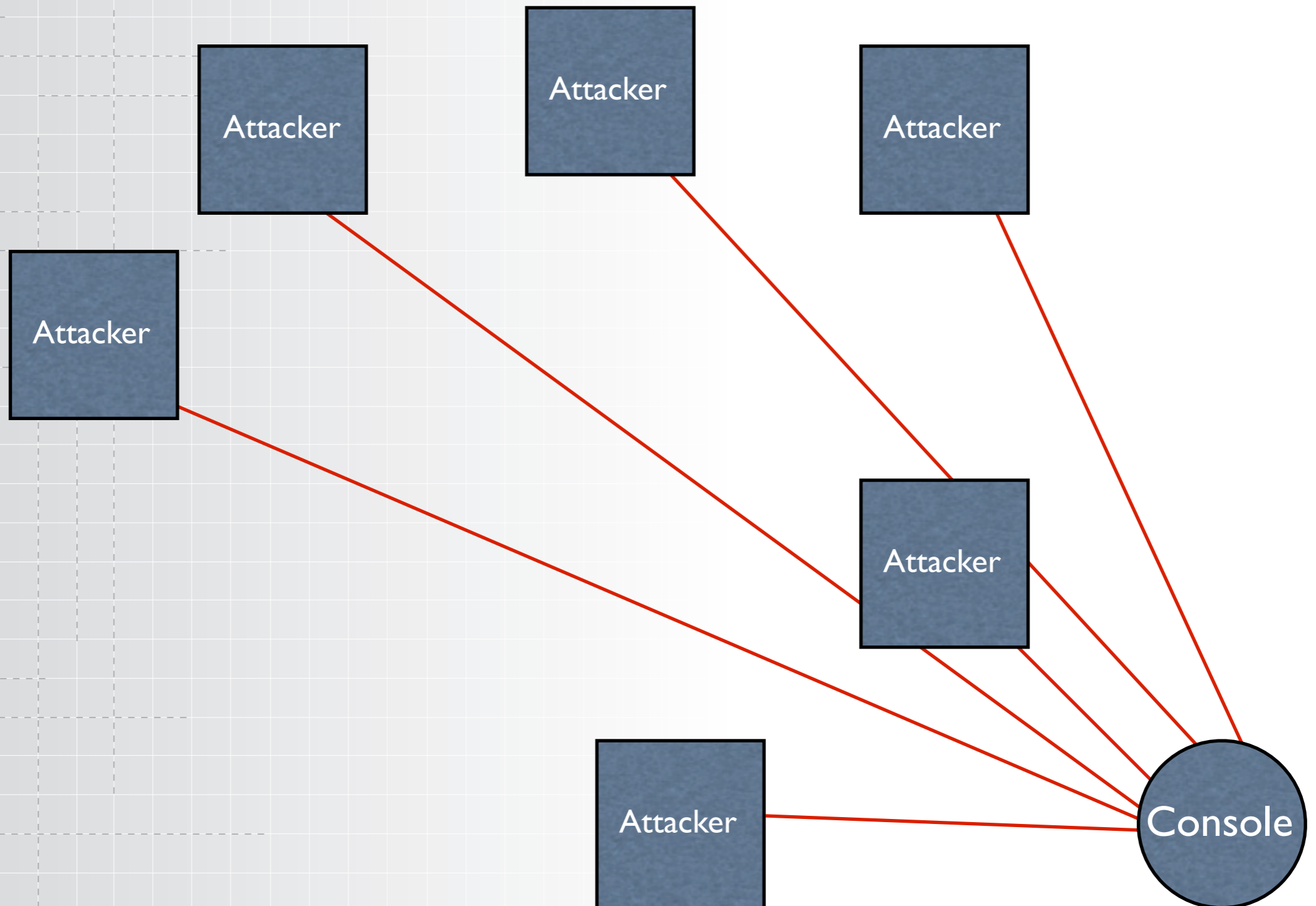
- Final refinement was introduction of “pulsing zombies”
- Like timed release but adds limit on length of attack
- This way it’s not only difficult to track back to the “console” but also to attackers as well. Each attacker only operates for a short time before going dormant for a while. Difficult to trace



pervasivetechlabs
AT INDIANA UNIVERSITY

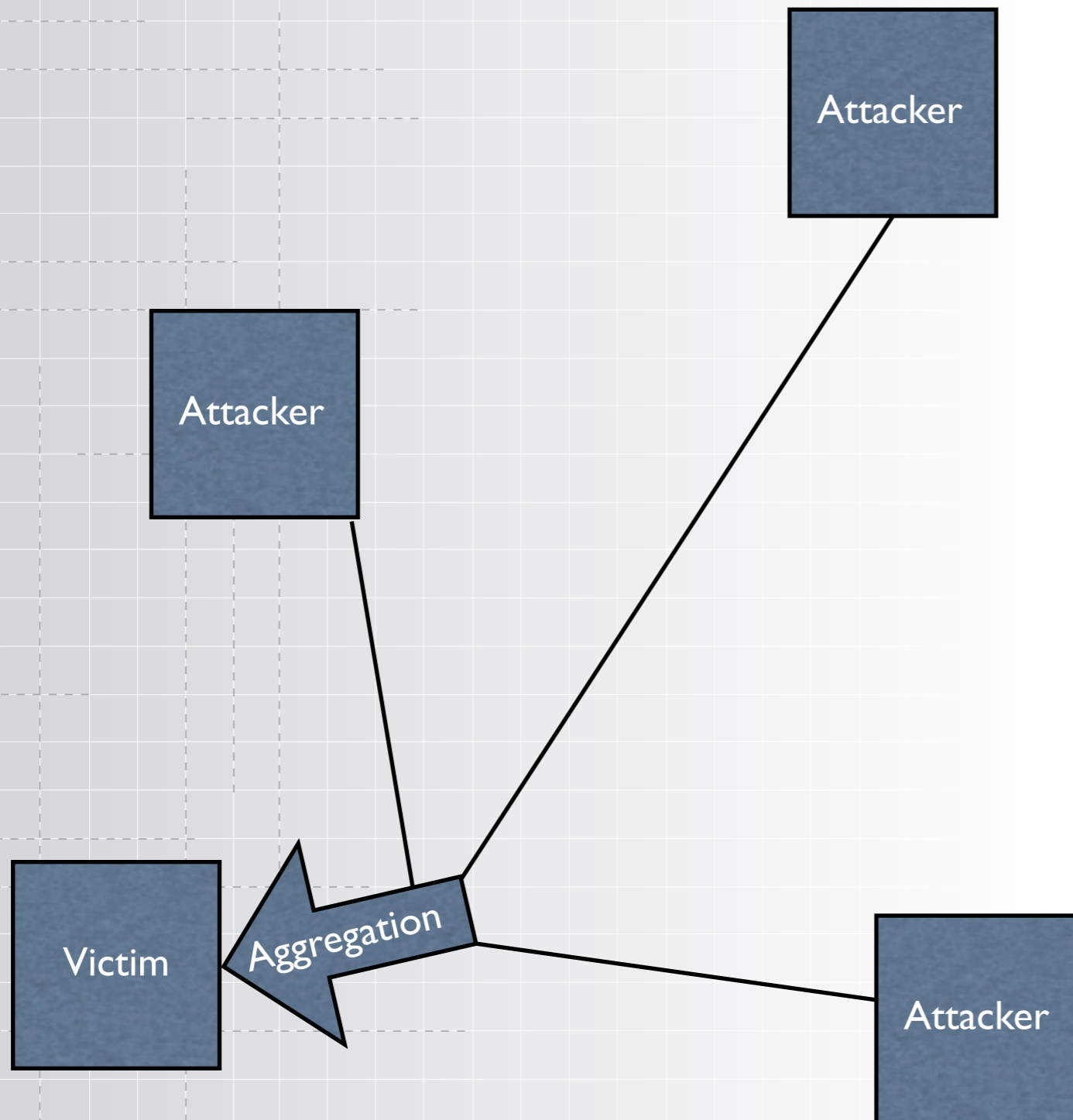
www.pervasivetechlabs.iu.edu

Zombie Setup





Zombie Attack

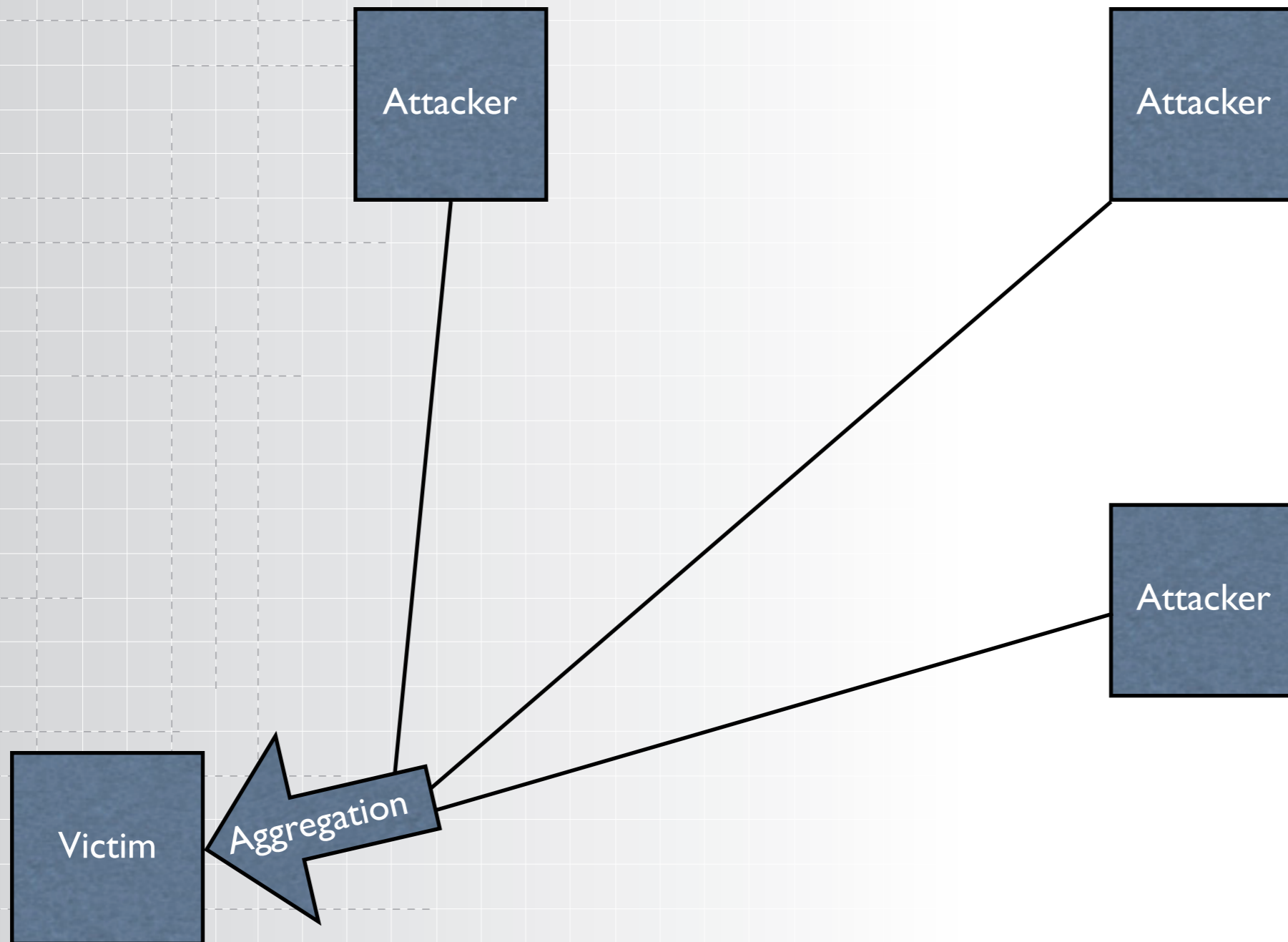




pervasivetechlabs
AT INDIANA UNIVERSITY

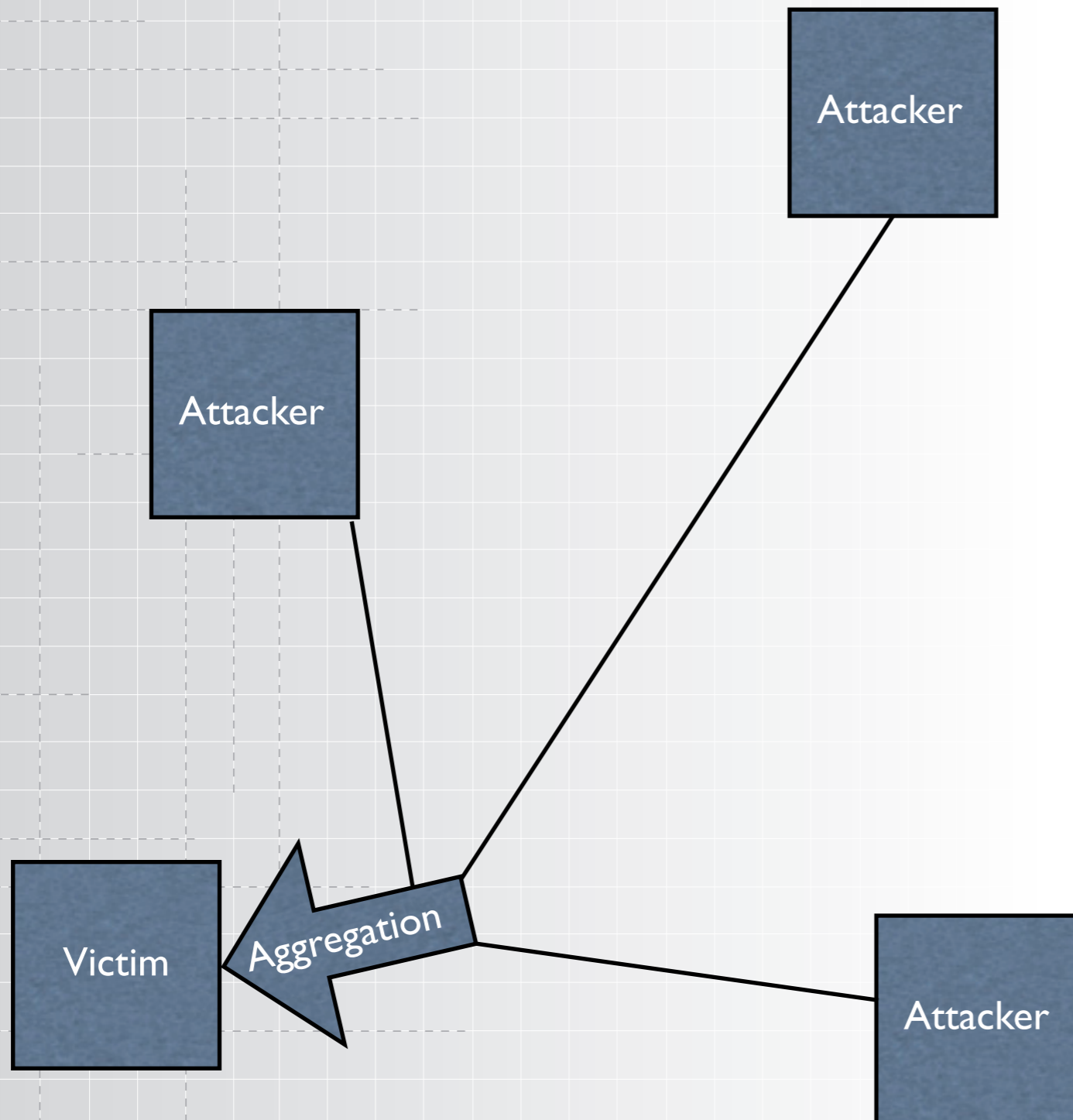
www.pervasivetechlabs.iu.edu

Zombie Attack





Zombie Attack

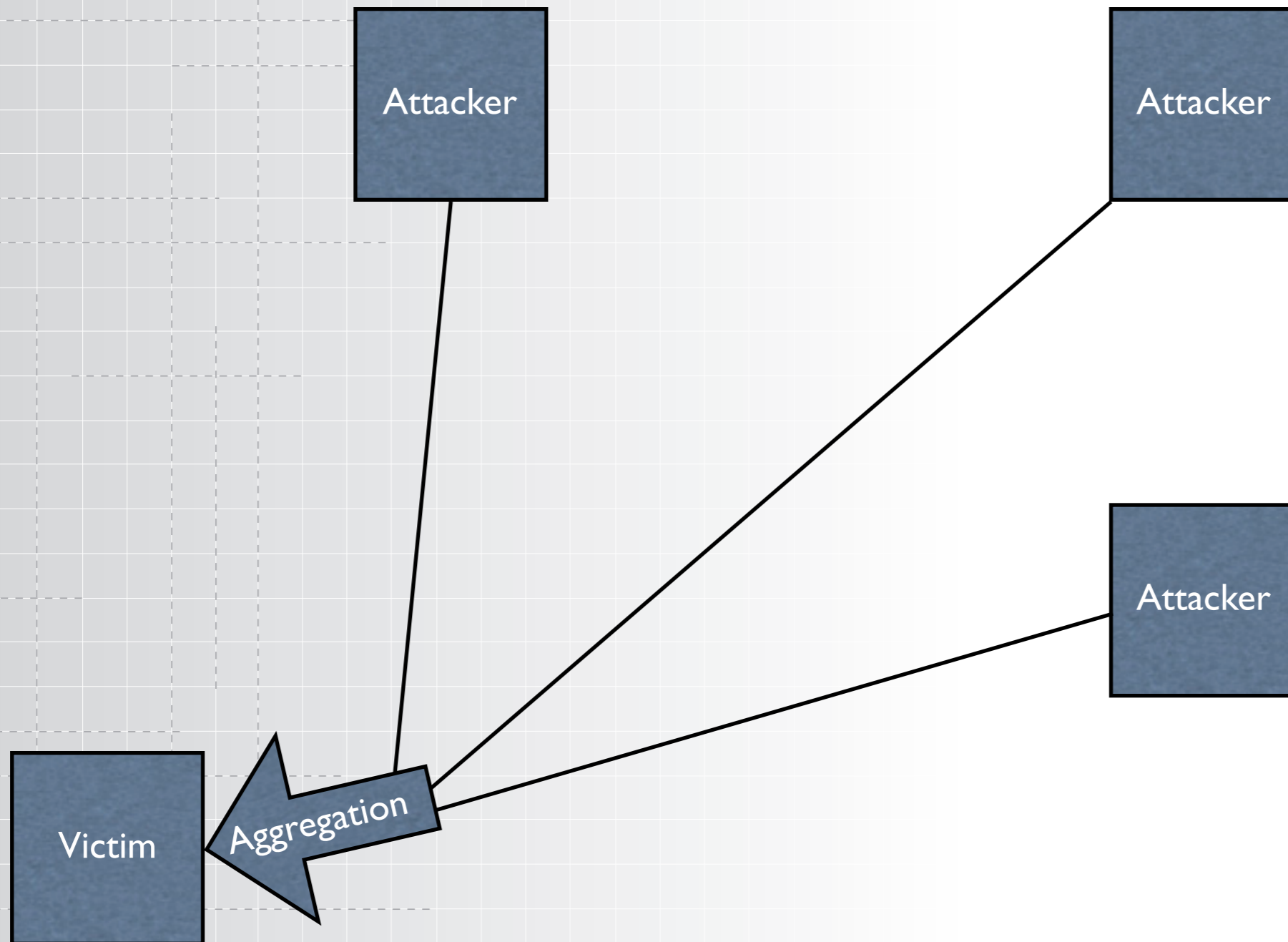




pervasivetechlabs
AT INDIANA UNIVERSITY

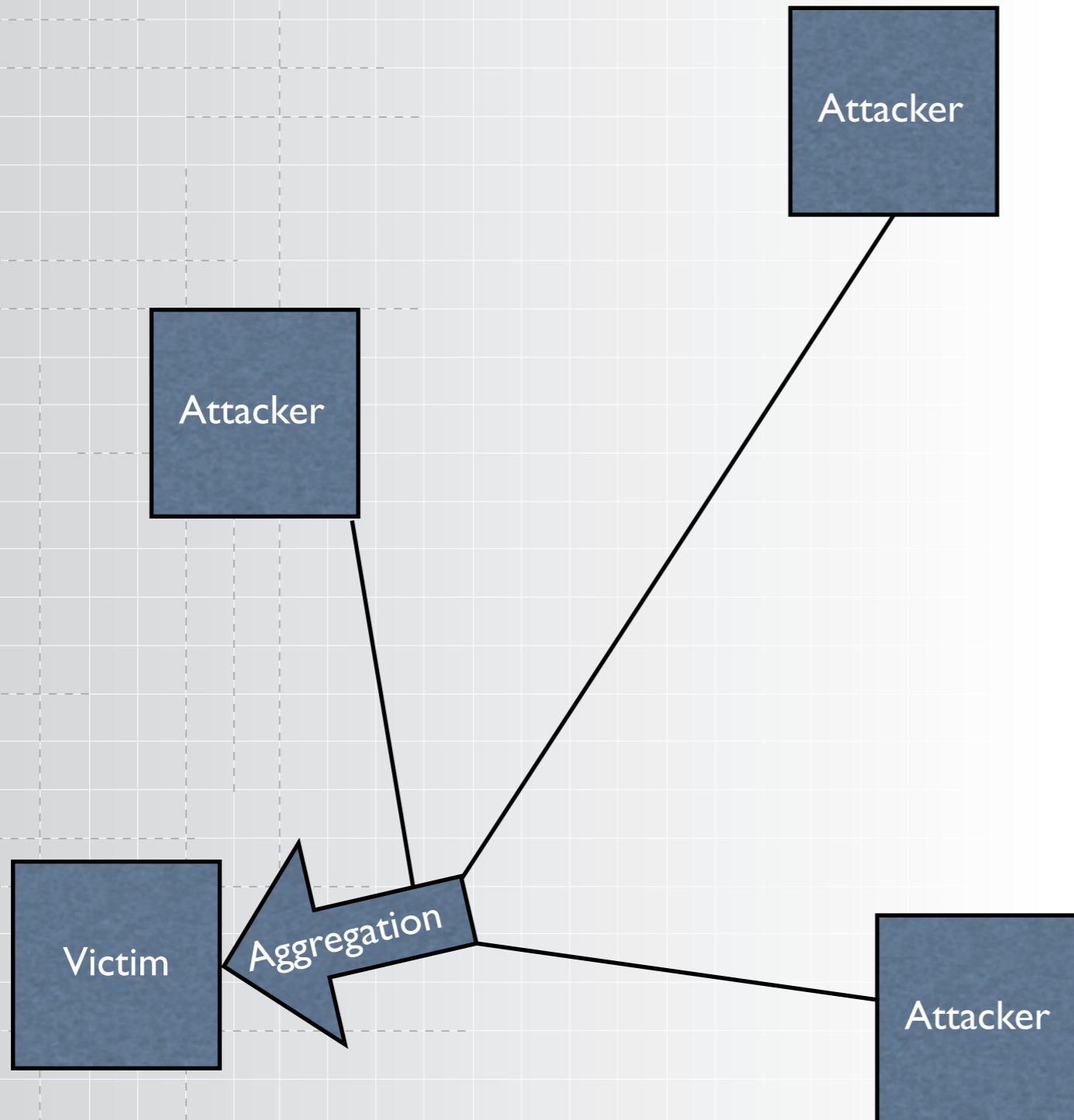
www.pervasivetechlabs.iu.edu

Zombie Attack





Zombie Attack

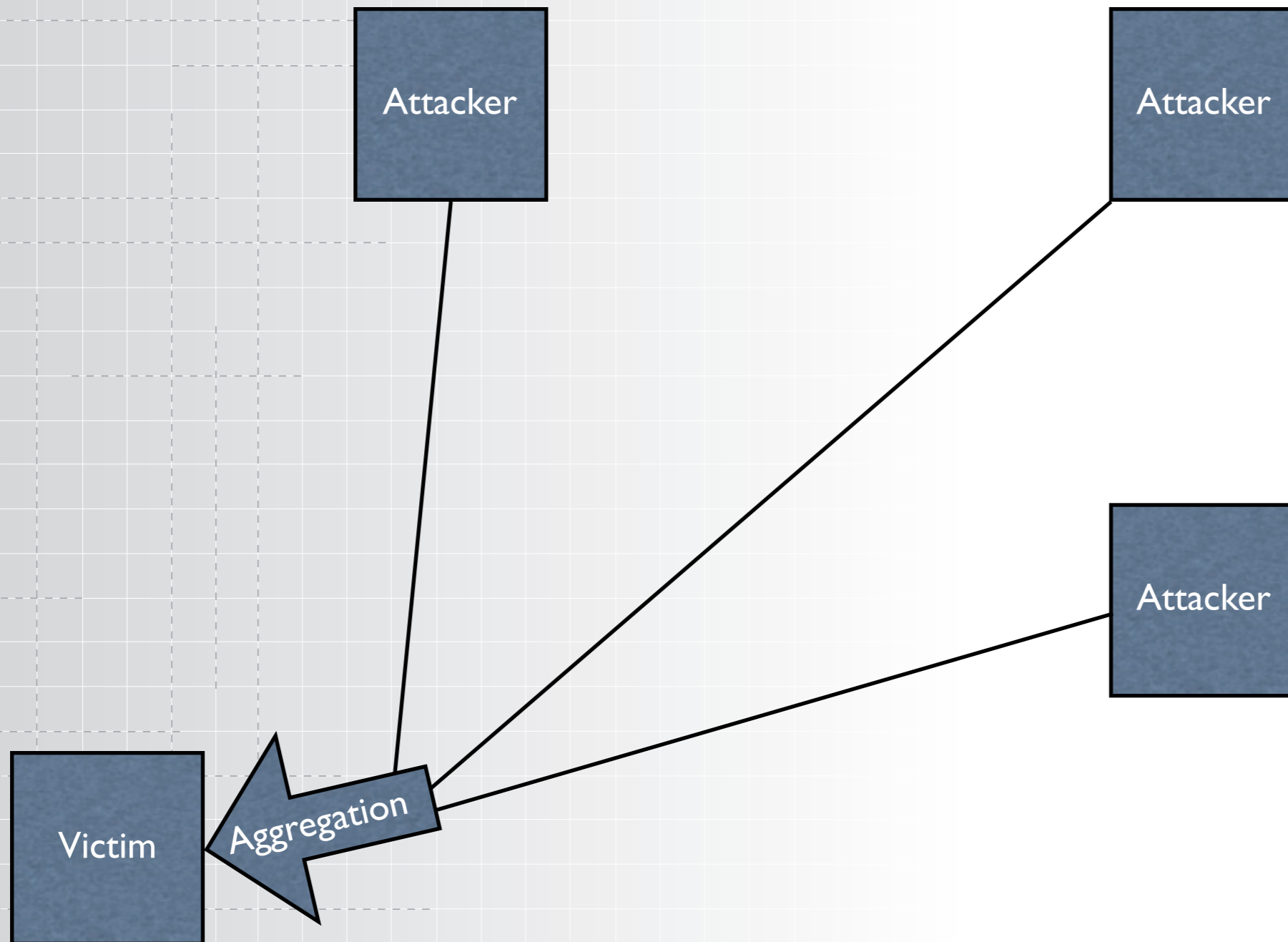




pervasivetechlabs
AT INDIANA UNIVERSITY

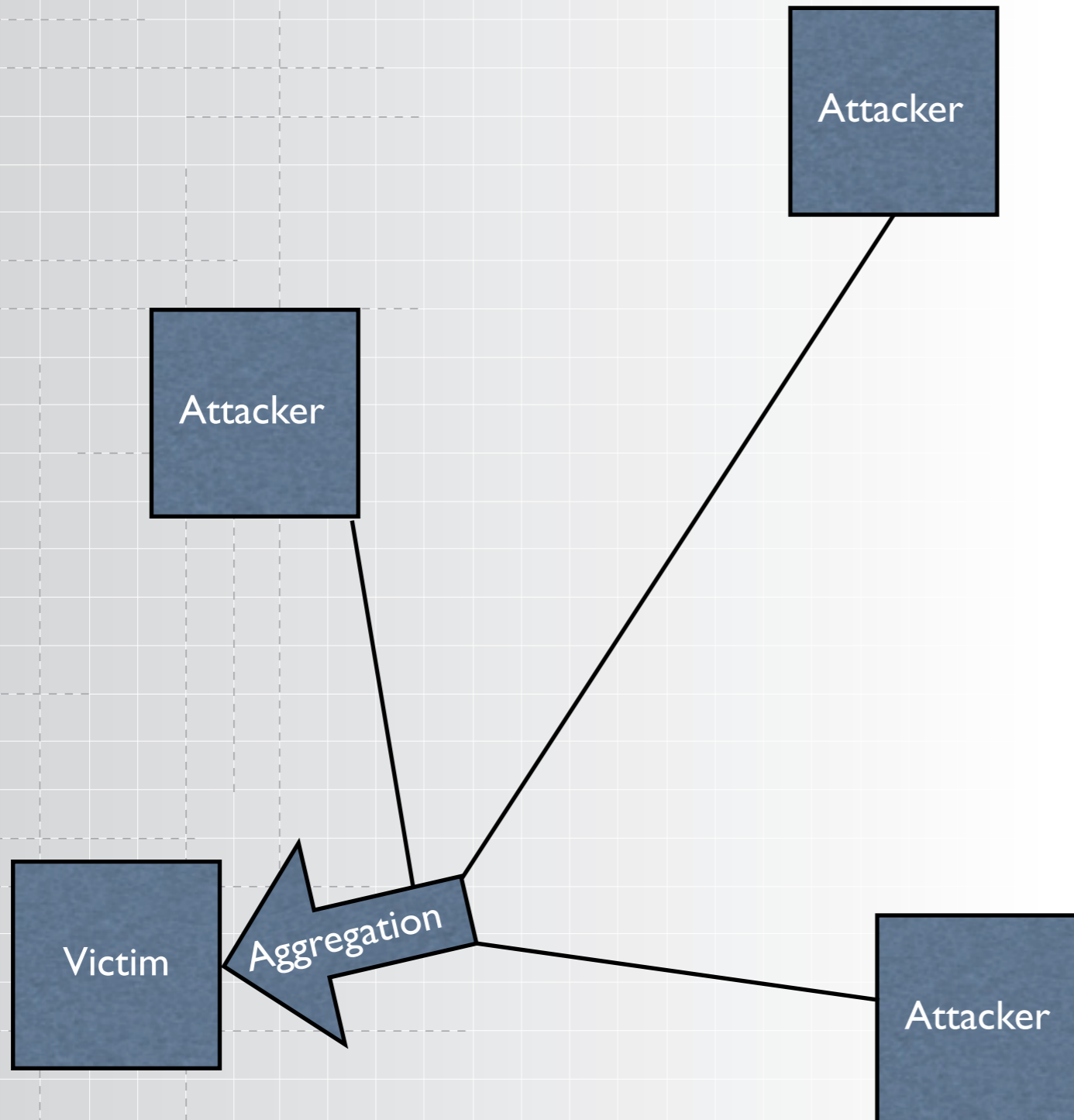
www.pervasivetechlabs.iu.edu

Zombie Attack



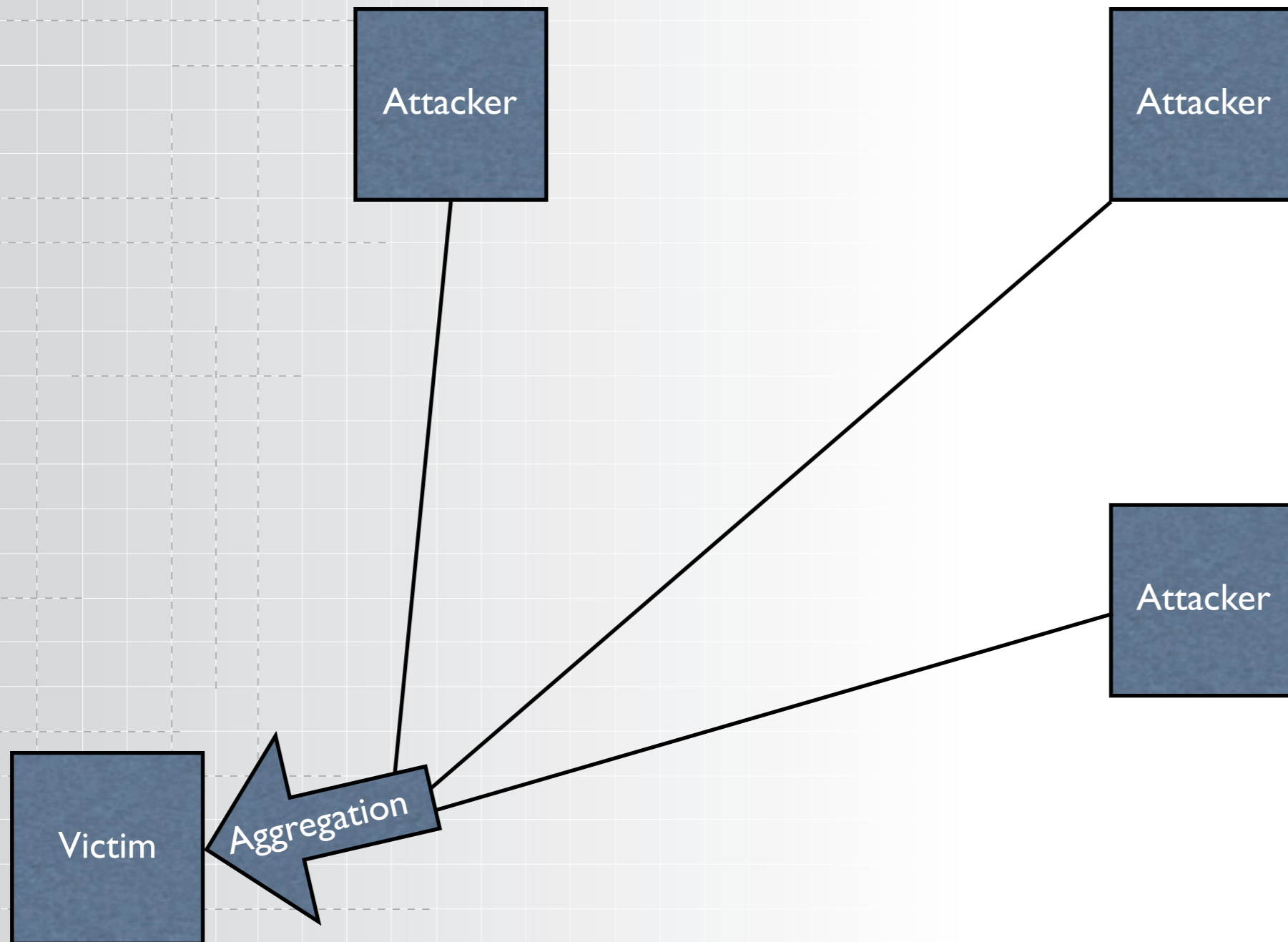


Zombie Attack





Zombie Attack

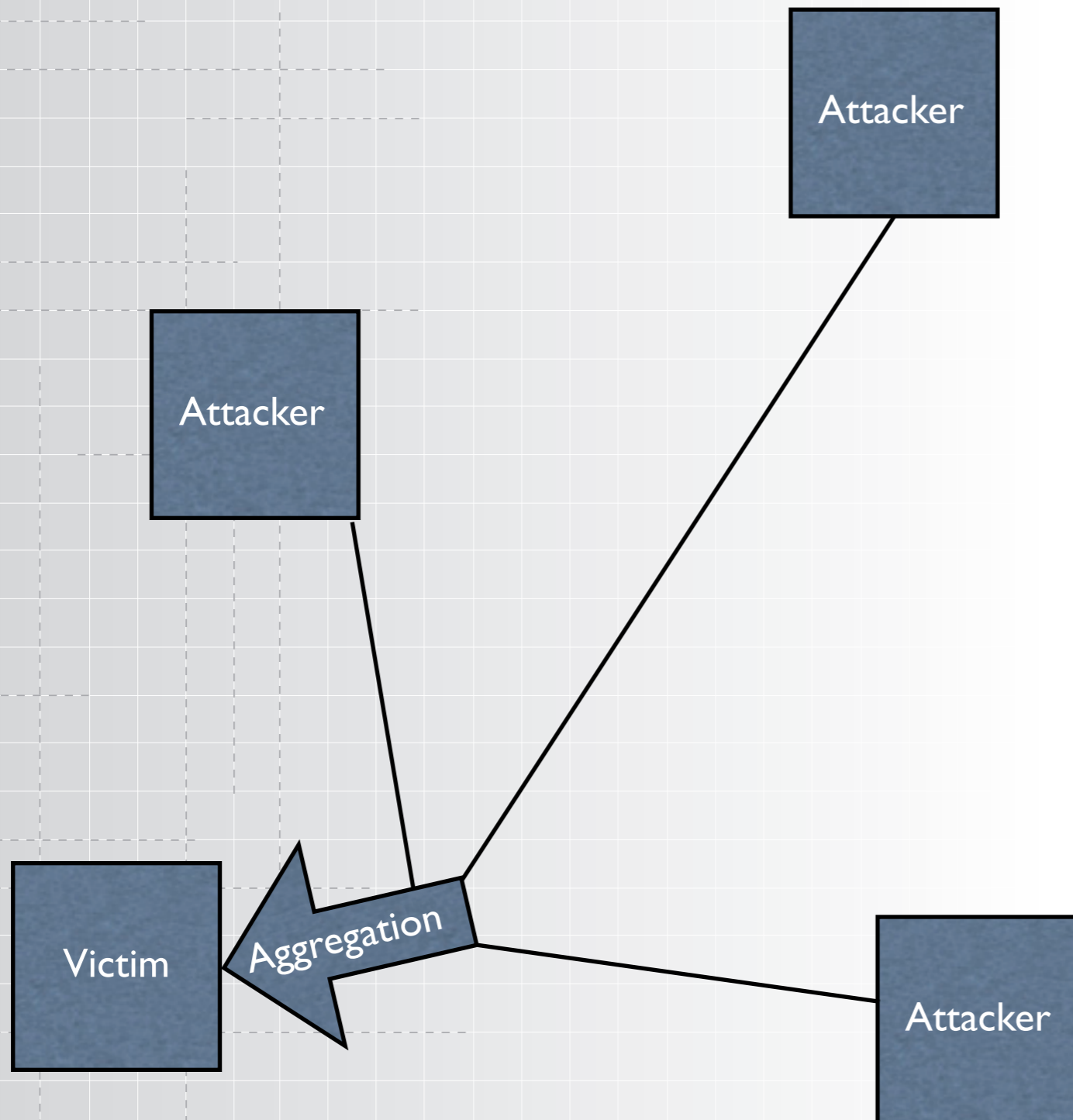




pervasivetechlabs
AT INDIANA UNIVERSITY

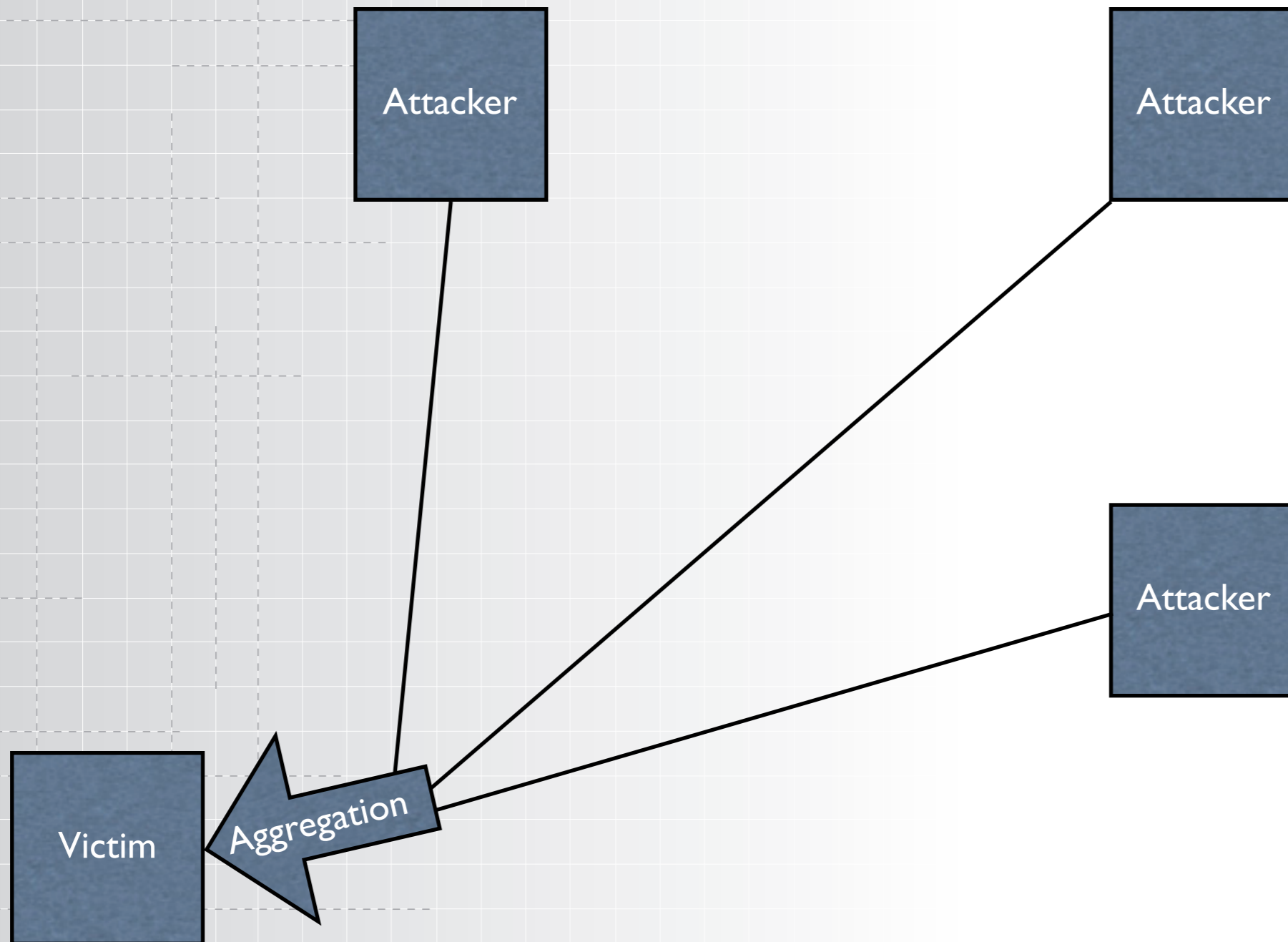
www.pervasivetechlabs.iu.edu

Zombie Attack





Zombie Attack

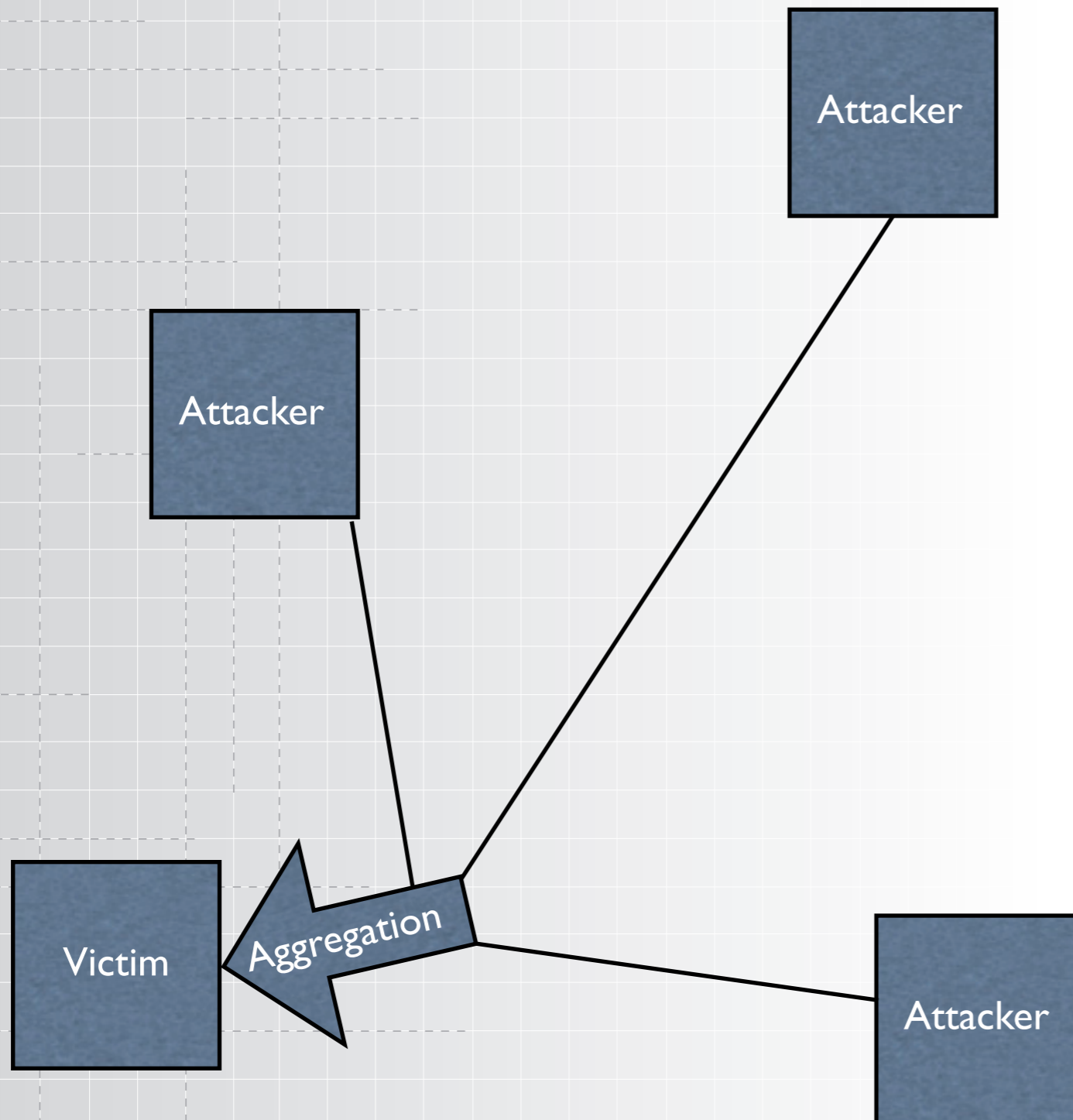




pervasivetechlabs
AT INDIANA UNIVERSITY

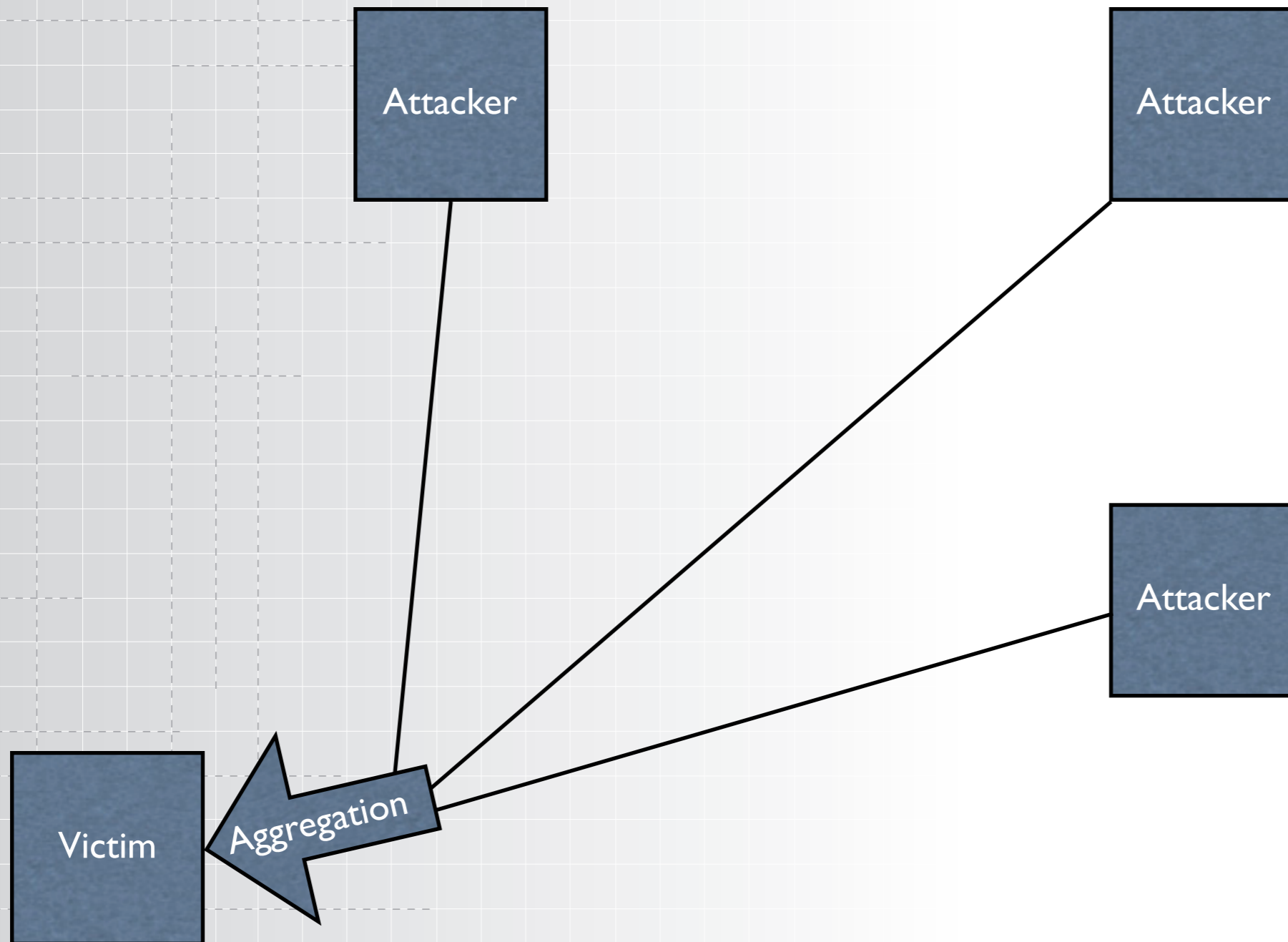
www.pervasivetechlabs.iu.edu

Zombie Attack





Zombie Attack





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Wrapup

- Evolution from DoS to DDoS to DDoS + “pulsing zombies”
- Concept of a “console”
- When compromise of systems is necessary and when not