How to Prevent a DDoS Attack

Very common attack
Not used to attack colleges

Company
- route unusual traffic elsewhere

People
- Deal with it, surely

Botnets

Worm propagates itself

Bot we under centralized control
- In facilities, control 6000
- IRC channel

DDoS: you need bigger pipe than victim
Botnet: lot of small pipes

How to take application offline

- Anything that creates a session with an initiation protocol
- Stop the initiation
  - like TCP SYN
HTTP: Request request send overload's requests

Spidrung: run through internal links to overload it

\[ \text{Thread} \]

\[ \text{request} \rightarrow \text{socket} \rightarrow \text{Thread} \]

Overload requests to slow down by threads

Reflector Attack: target through intermediate
Send attack to multiple intermediaries
Spoof the target IP
Intermediary attacks target with request

Options to stop: deal with it
Block intermediaries
- What if you need this intermediaries?

Infection Attack
-Spoof content
-600k requests per 120s response
-DNS causes this
DOES: not always accidental

- sometimes it just happens from lots of interest

Defense:

Security is the problem

ISP must ban IP3 but we also have that chain
- performance
  - attach traffic at center
  - hit reliable connection
- needs redundant paths
  - make things harder

Six Security: request response specificity

Instead of respond with aes
- send cookie
  - no information for this yet
- won't hold table

IPv6: Need for IP3
- need amplification
HTTP Flood
- Bombard with requests

Slower
Send HTTP requests that never complete
Legitimate requests are hard to organize data

折射
Attacker \rightarrow\textit{Intermediary} \rightarrow\textit{Target}
\rightarrow\textit{Intermediary}

Amplification win response is larger than request

Defense
Prevention: Get policy in place
Attacker Detection and Filtering
- rate control
Trace back and Identification
- hard with access
Analyze past attack for prediction