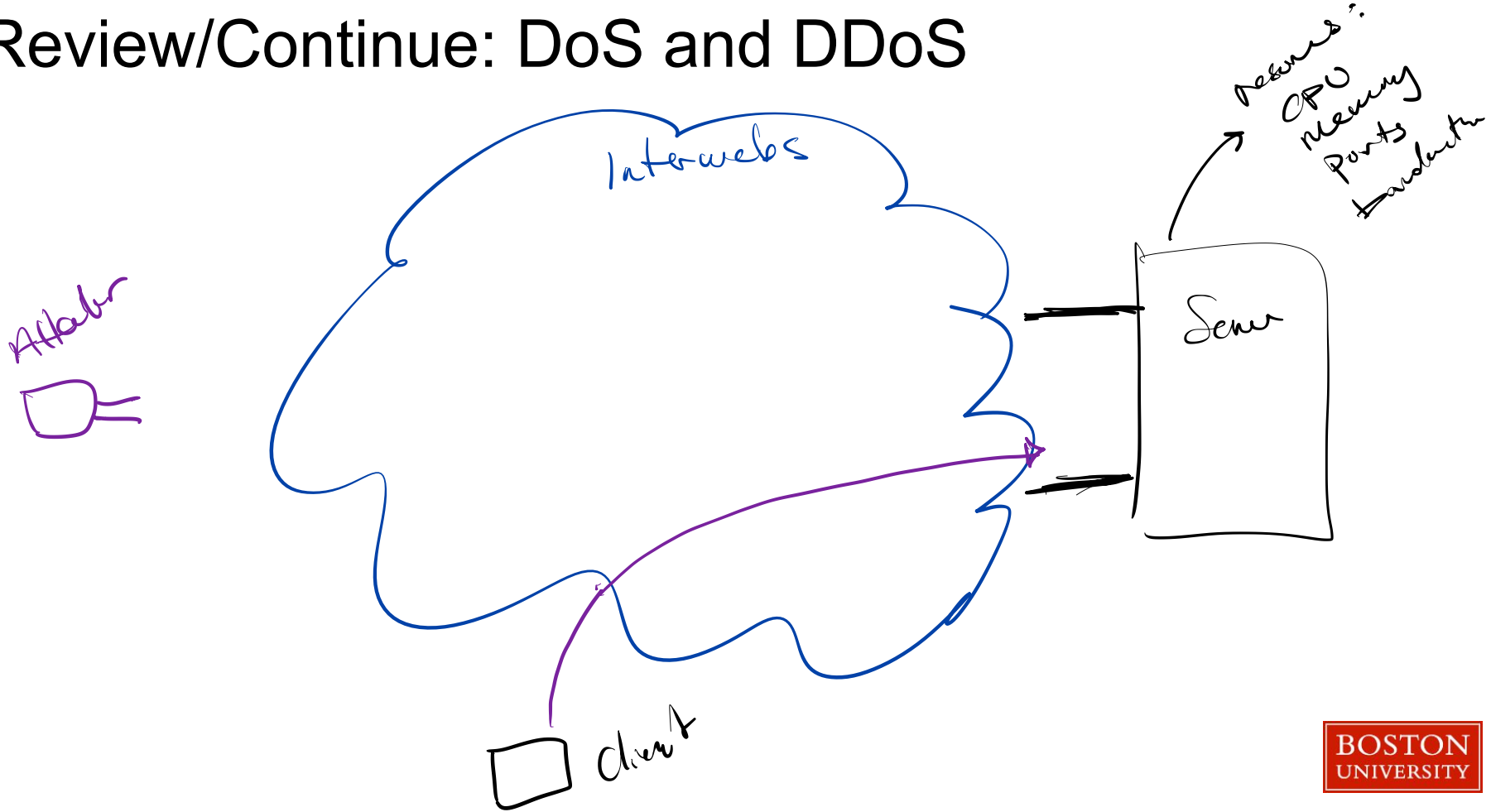
CS558 Network Security

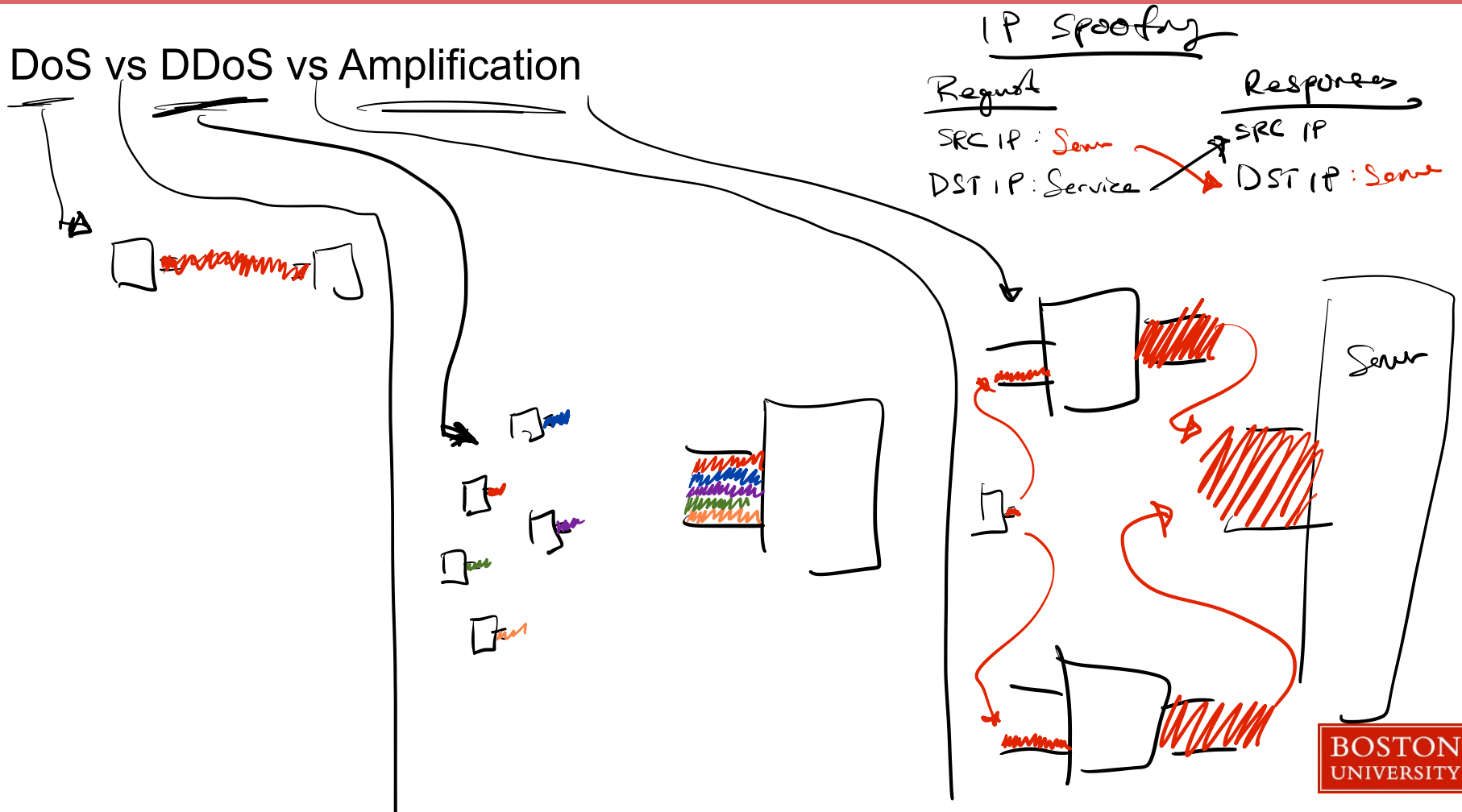
Lecture 9: DNS and DNSSec

BOSTON UNIVERSITY

Review/Continue: DoS and DDoS



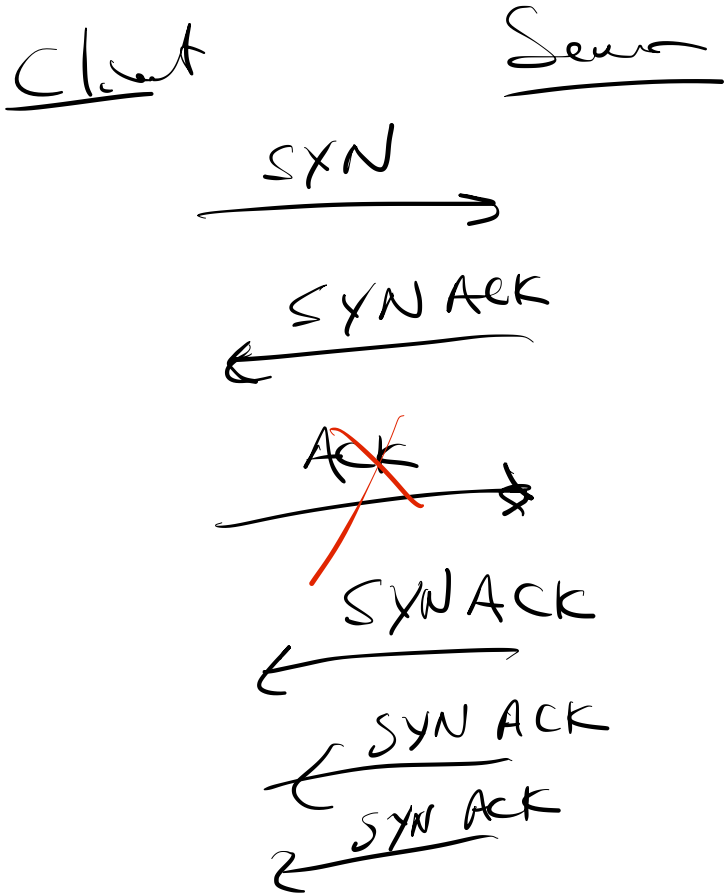
DoS vs DDoS vs Amplification

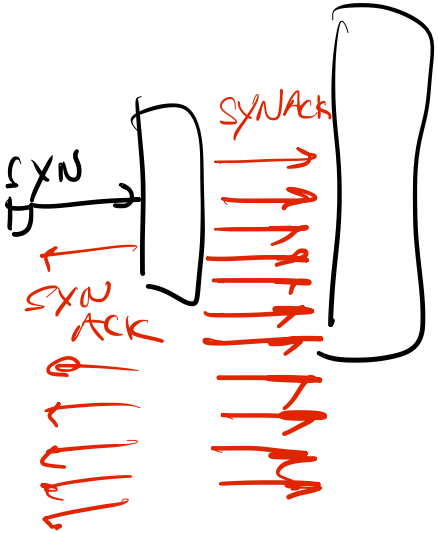


DDoS High Level Mitigation Strategies

- "real" and "fake traffic" → keep lists
- Don't reply times
- USe TCP
- DO some kind of montorg

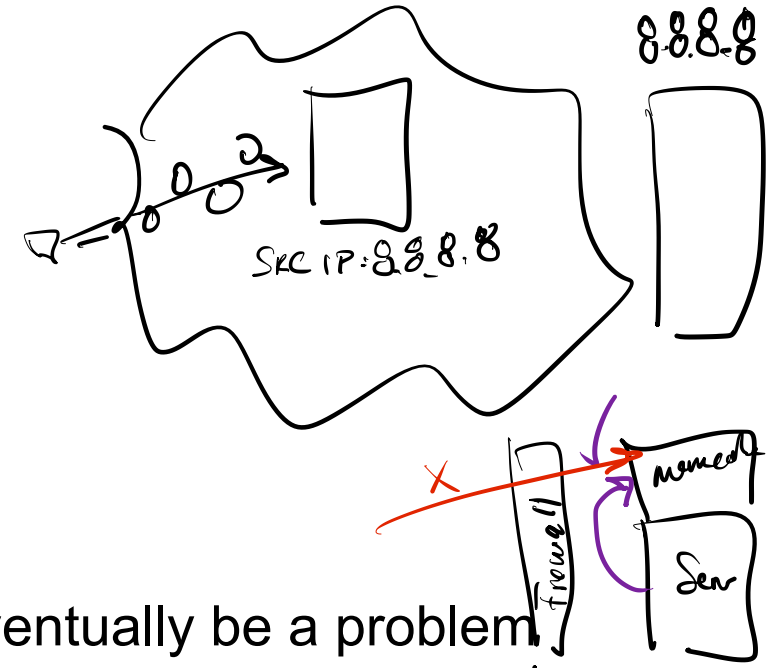
TCP





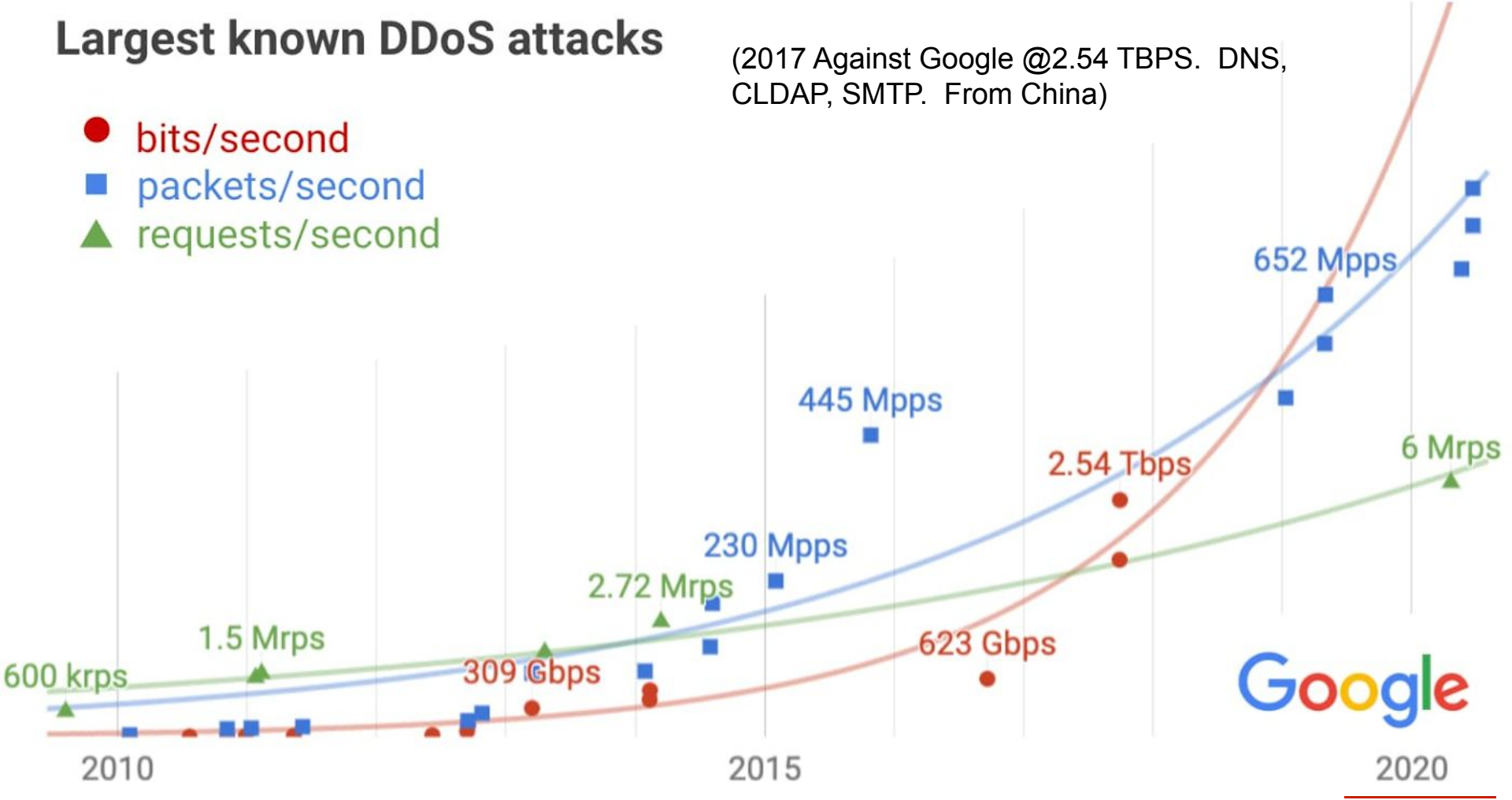
DDoS High Level Mitigation Strategies

- UDP can be a curse and a blessing
- IP Spoofing and Filtering
- Stateless Asymmetry
- Leaving stuff open by default may eventually be a problem
- Get someone to absorb traffic



Largest known DDoS attacks

(2017 Against Google @2.54 TBPS. DNS, CLDAP, SMTP. From China)



BIZ & IT —

DDoS attacks that crippled GitHub linked to Great Firewall of China

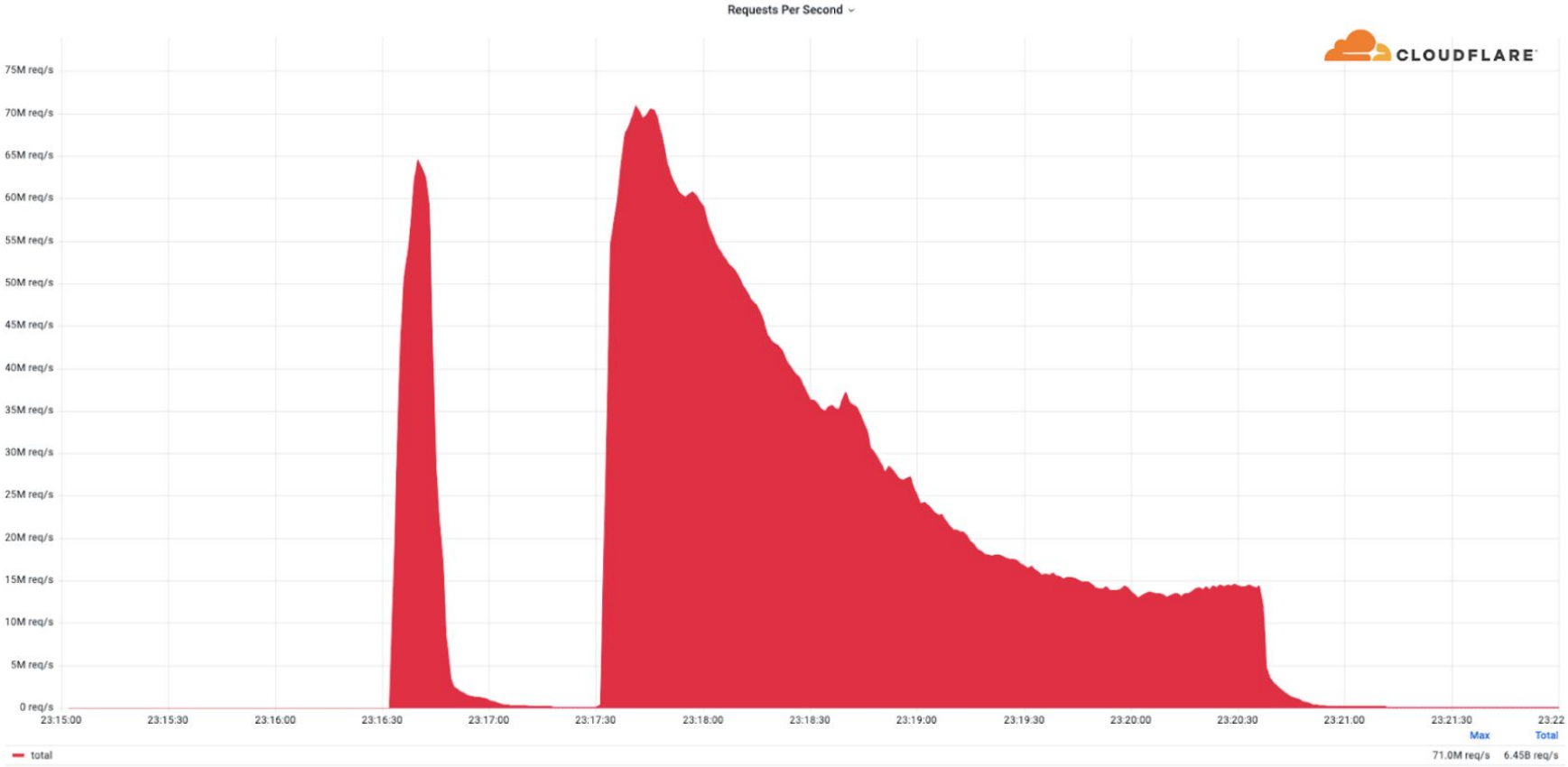
Whitehat hacker's traceroute wizzardry pinpoints origin of denial-of-service code.

DAN GOODIN - APR 2, 2015 10:31 PM UTC

Ryan McLaughlin

Bad javascript from Baidu Analytics

BOSTON UNIVERSITY



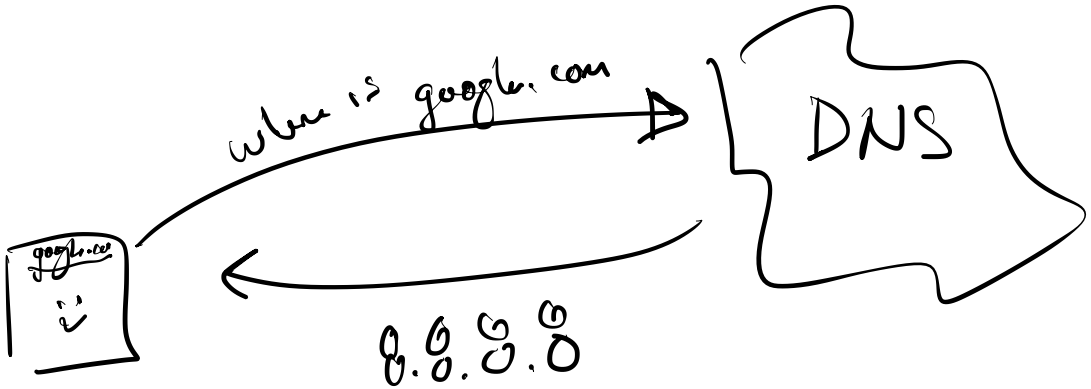
Record breaking attack: DDoS attack exceeding 71 million requests per second

DNS

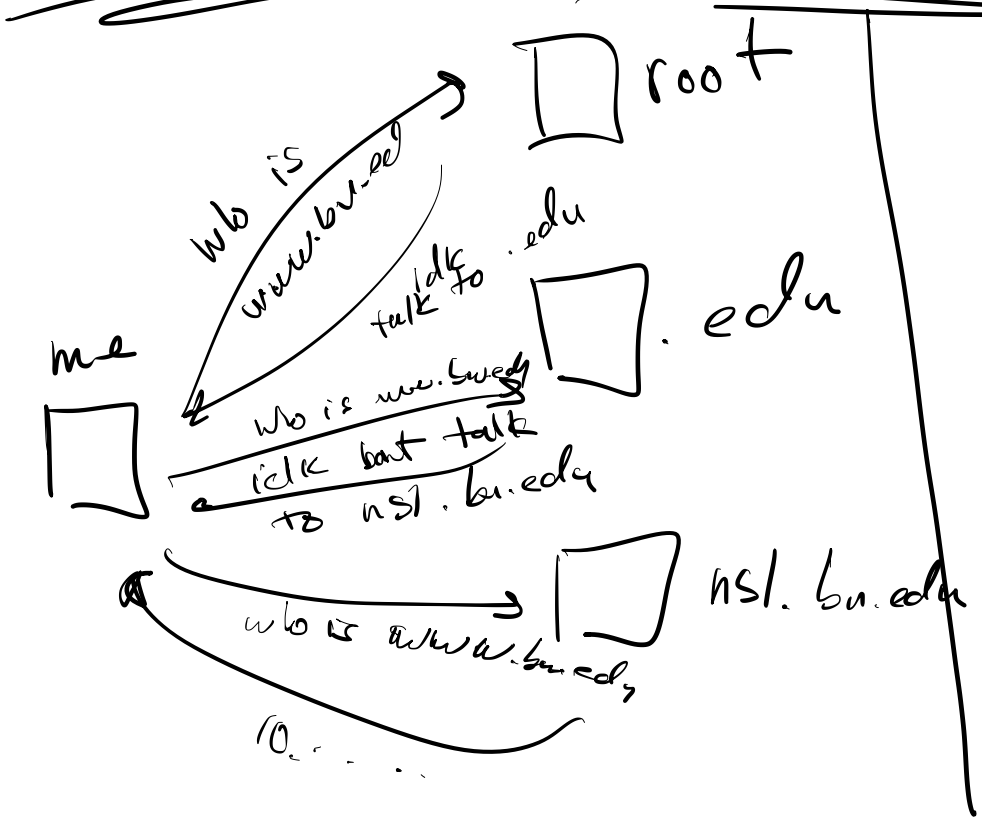
Domain Names
"www.bu.edu"

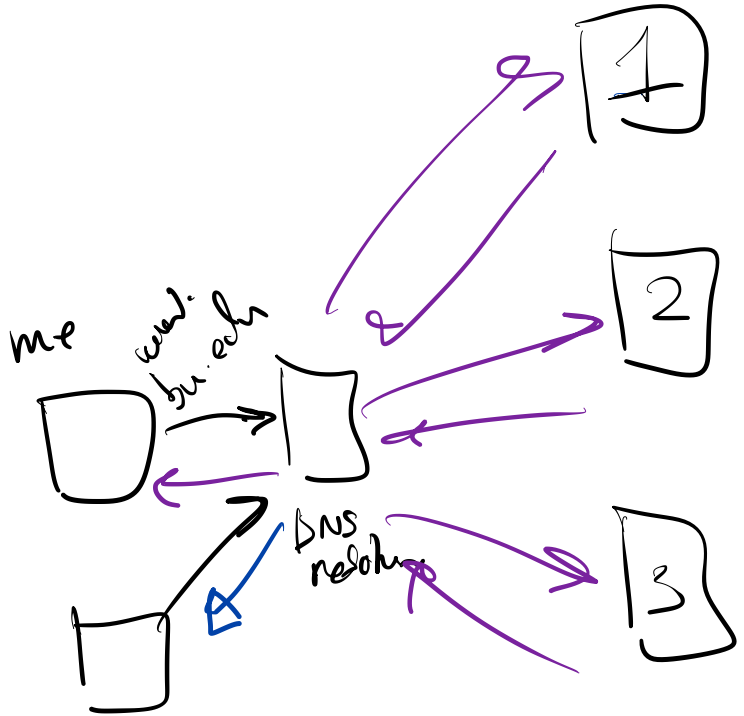
IP address
162.152.1.6

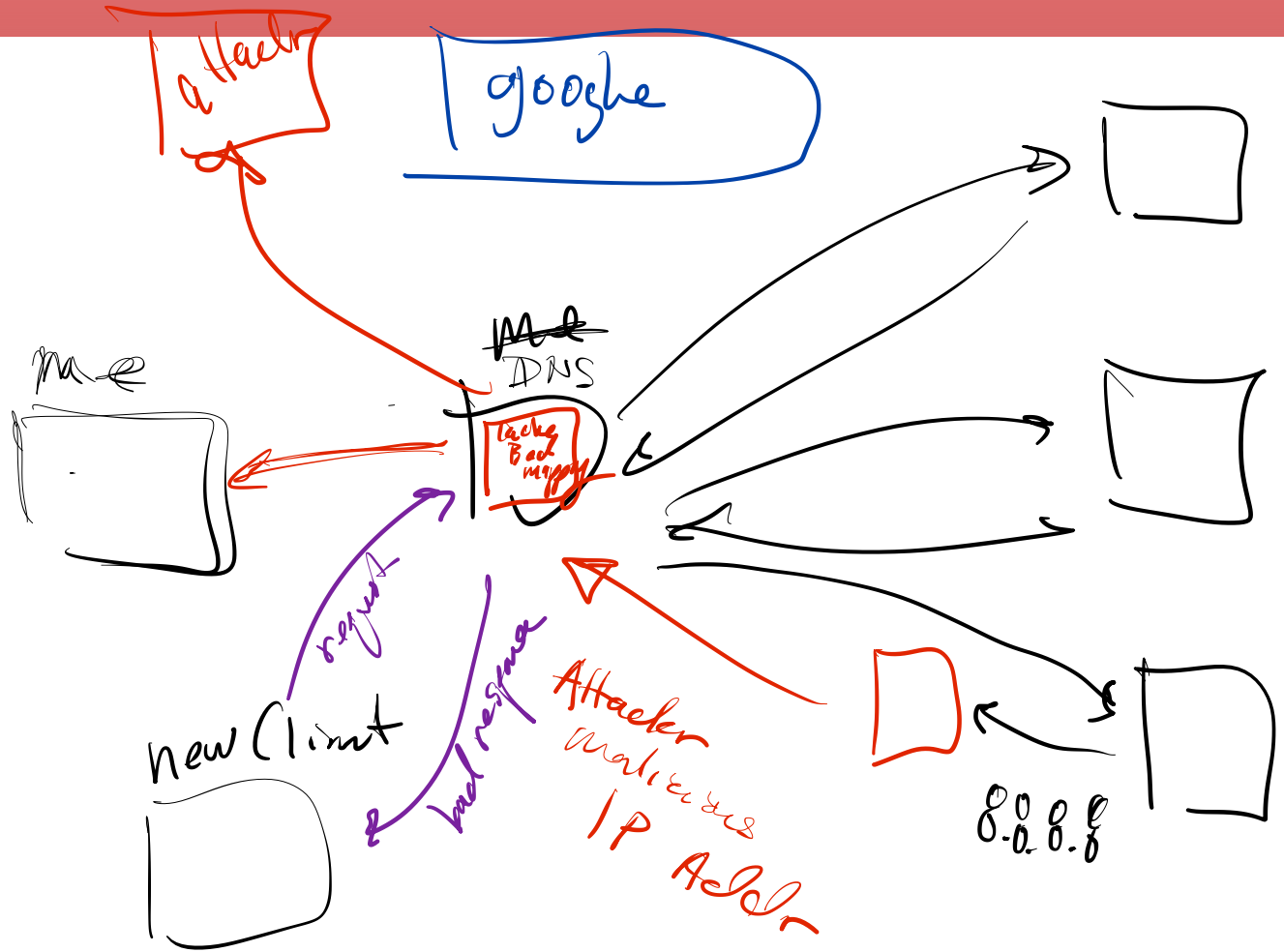
Scalability
Dynamic
Human Load @ #.

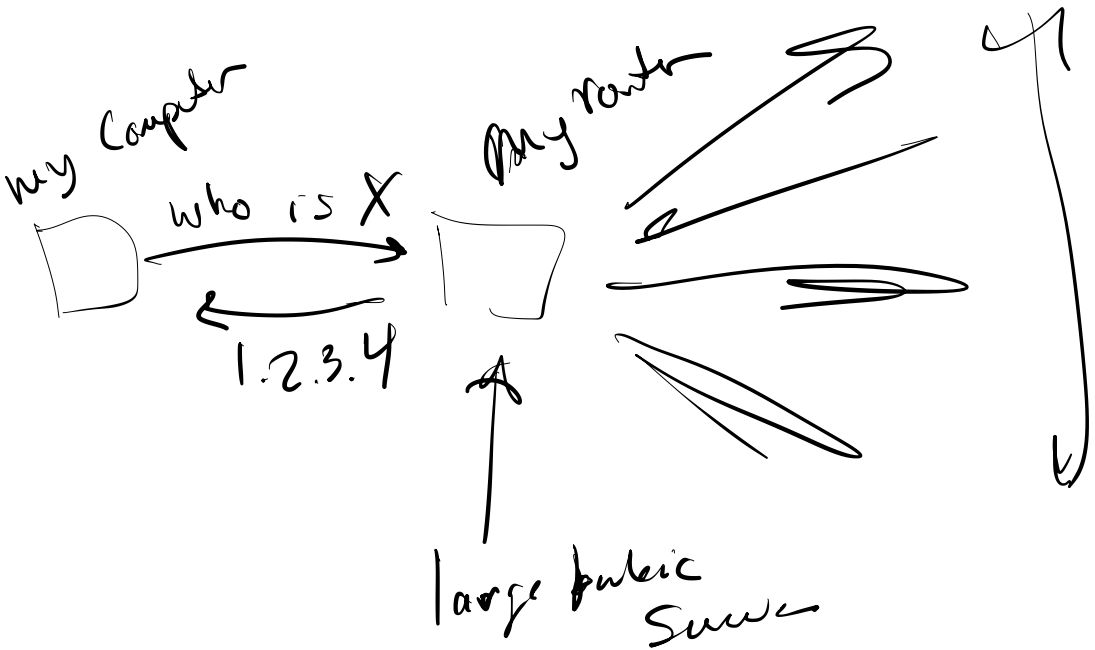


DNS Iterative/Recursive Resolving









NEWS

China's Great Firewall spreads overseas

By Robert McMillan

IDG News Service | MAR 25, 2010 4:19 PM PST

A networking error has caused computers in Chile and the U.S. to come under the control of the Great Firewall of China, redirecting Facebook, Twitter, and YouTube users to Chinese servers.