DOS AND DDOS CONT.
Lecture 15a

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

August 19, 2021

Source of some slides: **CMU**, **Stanford University**, and **University of Twente**

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

GENERAL COUNTERMEASURES

- Protocol hardening
- Patch your machine
- Firewall
  - Filter out packets entering local network from the Internet that have a source address of the local network
- Intrusion Detection Systems (IDS)

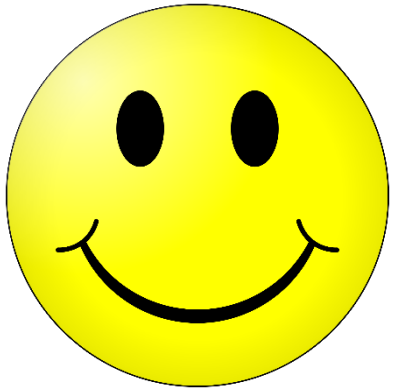
SUMMARY

- Information can be gathered using port scanning
- For mounting DoS: Use brute-forcing or semantic attacks
- A single machine can bring down multiple servers
- Use Content Delivery Network (CDN) services for mitigating DoS and DDoS
  - E.g., CloudFlare

RESOURCES

- Read Chapter 10 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

- Terrance A. Roebuck,
  Network Security: DoS vs DDoS Attacks
  Available: http://www.crime-research.org/articles/network-security-dos-ddos-attacks



Questions?

Thanks for your attention!