

CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Countermeasures and Famous DDoS Attacks



Video Summary

- DDoS Prevention, Detection, and Response
- Defending DDoS
- Famous DDoS Attacks
- Digital Attack Map



Constructing Attack Network

- ▶ Attacker must get many slave hosts under its control
 - ▶ Infect the hosts with zombie software
1. Create software that will perform the attacks. This should:
 - ▶ Be able to run on different hardware architectures and OSes
 - ▶ Hide, that is not be noticeable to the normal user of the zombie host
 - ▶ Be able to be contacted by attacker to trigger an attack
 2. Identify vulnerability (bug) in large number of systems, in order to install the zombie software



DDoS Attack Prevention, Detection, Response

- ▶ Prevention

- ▶ Allocate backup resources and modify protocols that are less vulnerable to attacks
- ▶ Aim is to still be able to provide some service when under DDoS attack

- ▶ Detection

- ▶ Aim to quickly detect an attack and respond
- ▶ Detection involves looking for suspicious patterns of traffic

- ▶ Response

- ▶ Aim to identify attackers so can apply technical or legal measures to prevent
- ▶ Cannot prevent current attack; but may prevent future attacks



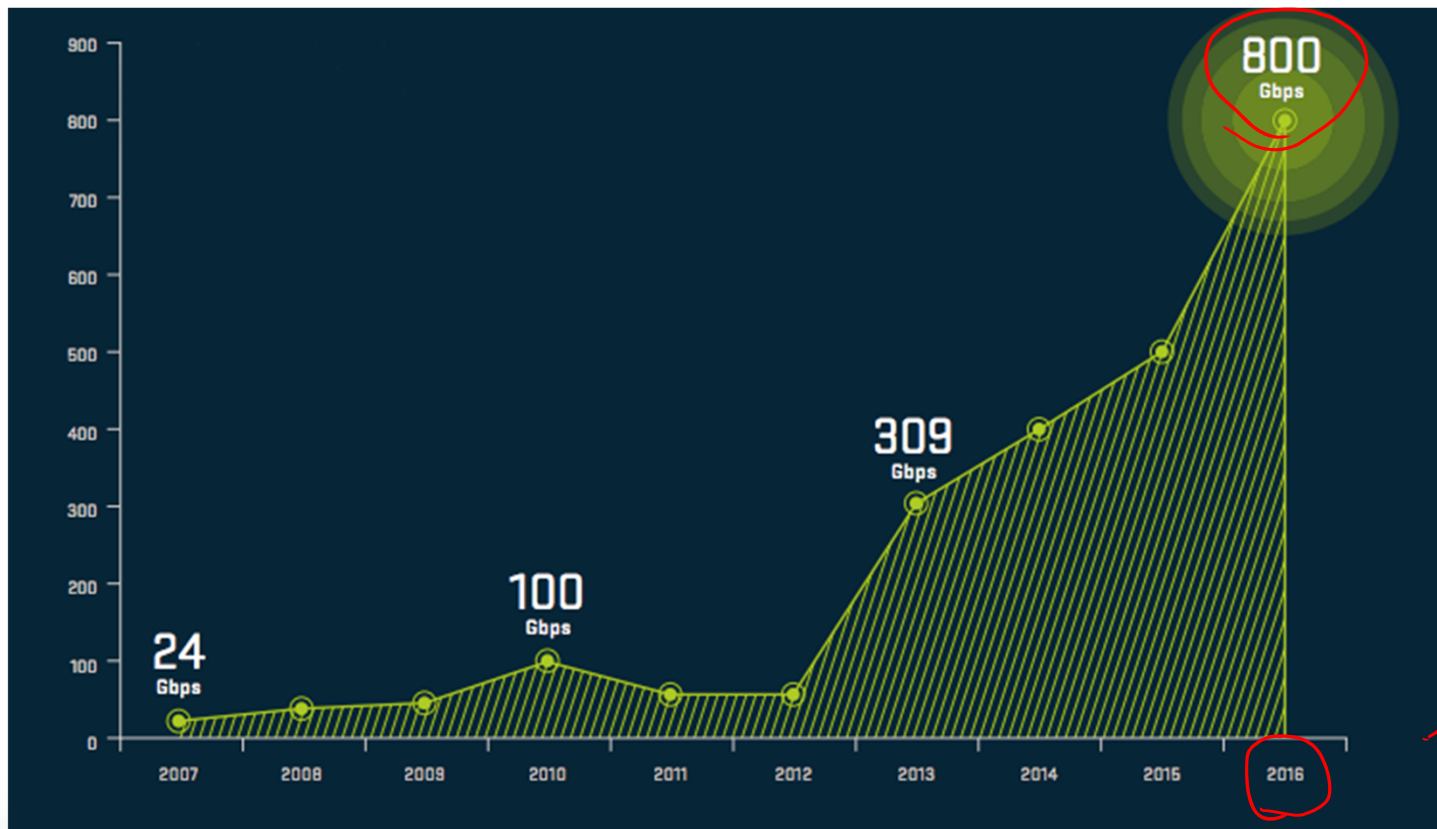
HOW TO DEFEND

- Firewalls - can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.
- Switches - Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding to detect and remediate denial of service attacks
- Routers - If you add rules to take flow statistics out of the router during the DoS attacks, they further slow down and complicate the matter



ATTACK SIZE IN GBITS-PER-SECOND

1TB



2018


Attack using Trin00

- In August 1999, network of > 2,200 systems took University of Minnesota offline for 3 days
 - scan for known vulnerabilities, then attack with UDP traffic
 - Source addresses were not spoofed, so systems running the offending daemons were contacted. However, the attacker responded simply by introducing new daemon machines into the attack.



Most Famous/Recent DDoS Attacks

In recent years, DDoS attacks have only been increasing in both frequency and severity. Here, we'll explore five of the largest and most famous DDoS attacks.

- 
1. GitHub
 2. Occupy Central Hong Kong
 3. CloudFlare
 4. Spamhaus
 5. U.S. Banks



Most Famous DDoS Attacks

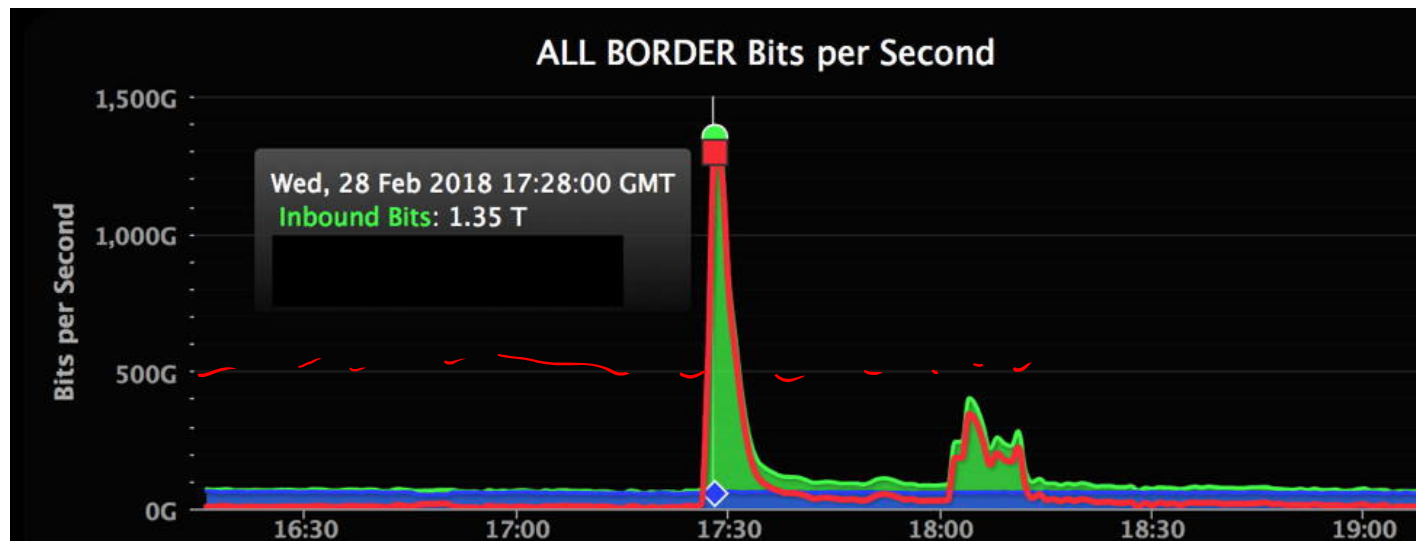
➤ GitHub: 1.35 Tbps

- On Feb. 28, 2018, GitHub was hit with a sudden traffic that clocked in at 1.35 Tbps.
- If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking.
- According to [GitHub](#), the traffic was traced back to “over a thousand different autonomous systems across tens of thousands of unique endpoints.”



Most Famous DDoS Attacks

➤ GitHub: 1.35 Tbps



Most Famous DDoS Attacks

➤ Occupy Central, Hong Kong: 500 Gbps

- The [PopVote DDoS attack](#) was carried out in 2014 and targeted the Hong Kong-based grassroots movement known as Occupy Central. The movement was campaigning for a more democratic voting system.



Authorities hit Hong Kong protestors with tear gas.

The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites

Most Famous DDoS Attacks

➤ Occupy Central, Hong Kong: 500 Gps

- In response to their activities, attacker(s) sent large amounts of traffic to three of Occupy Central's web hosting services, as well as two independent sites, PopVote, an online mock election site, and Apple Daily.
- The attack flooded servers with packets appeared as legitimate traffic, and was executed with five botnets. This resulted in peak traffic levels of 500 Gbps.



Most Famous DDoS Attacks

➤ CloudFlare: 400 Gbps

- In 2014, security provider and content delivery network CloudFlare was slammed by approximately 400 Gbps of traffic.
- The attack was directed at a single CloudFlare customer and targeted servers in Europe and was launched with the help of a vulnerability in the Network Time Protocol (NTP), a networking protocol for computer clock synchronization.
- Even though the attack was directed at just one of CloudFlare's customers, it was so powerful that it affected CloudFlare's own network.



Most Famous DDoS Attacks

➤ Spamhaus: 300 Gbps

- Although Spamhaus, as an anti-spam organization, was and is regularly threatened and attacked.
- This DDoS attack was large enough to knock their website offline, as well as part of their email services.
- The attack was traced to a member of a Dutch company named Cyberbunker.



Most Famous DDoS Attacks

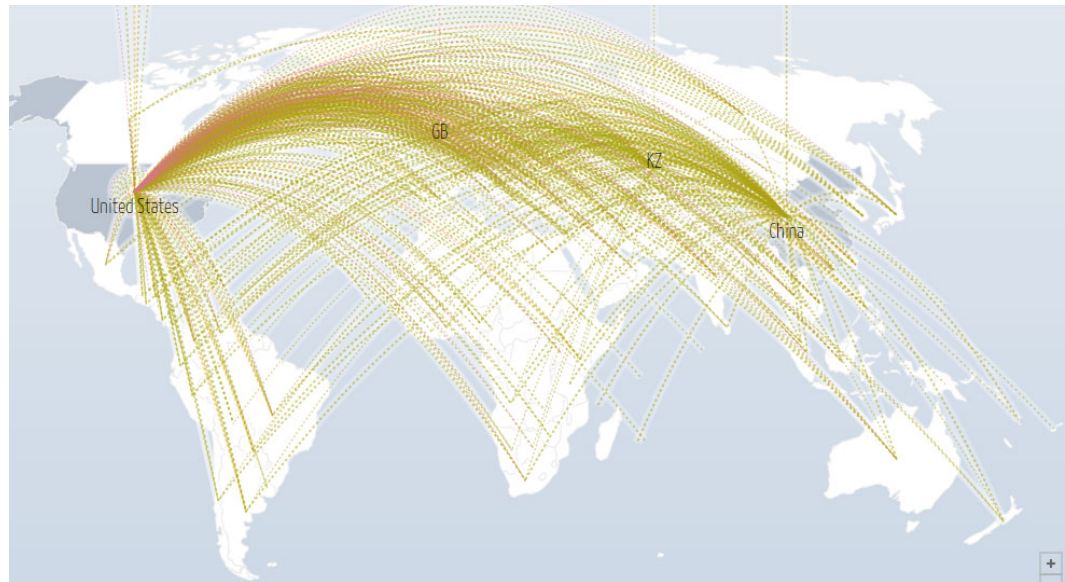
➤ U.S. Banks: 60 Gbps

- In 2012, six U.S. banks were targeted by a string of DDoS attacks.
- The victims were: **Bank of America, JP Morgan Chase, U.S. Bancorp, Citigroup and PNC Bank.**
- The attack was carried out by hundreds of hijacked servers, which each created peak floods of more than 60 gigabits of traffic per second.
- Rather than trying to execute one attack and then backing down, the attackers flooded their targets with different DDoS methods in order to find one that worked.
- So, even if a bank was equipped to deal with a few types of DDoS attacks, they were helpless against other types.



Digital Attack Map

<https://www.digitalattackmap.com/>



Video Summary

- DDoS Prevention, Detection, and Response
- Defending DDoS
- Famous DDoS Attacks
- Digital Attack Map

