RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

Information Security

SECURING WEB SERVICES FROM DOS ATTACKS

Bhagyashree Parkar
Parvesh Kopparapu

Abstract

- Web Services (WS) Technology has become the main reference architecture for heterogeneous systems.
- Companies nowadays are vulnerable to a lot of Web Services attacks as it is very important for them to use the internet for communication.
- Our main objective is to present a systematic review of the studies of web service security, attacks, and how to prevent them.

Attacks

- Denial of Services (DoS) attack
- SQL injections
- XML injections
- Cross-Site Scripting (XSS)
- Xpath
- Spoofing

These attacks make it very difficult to secure confidential data stored on computers and servers while exchanging data during operation over a network.

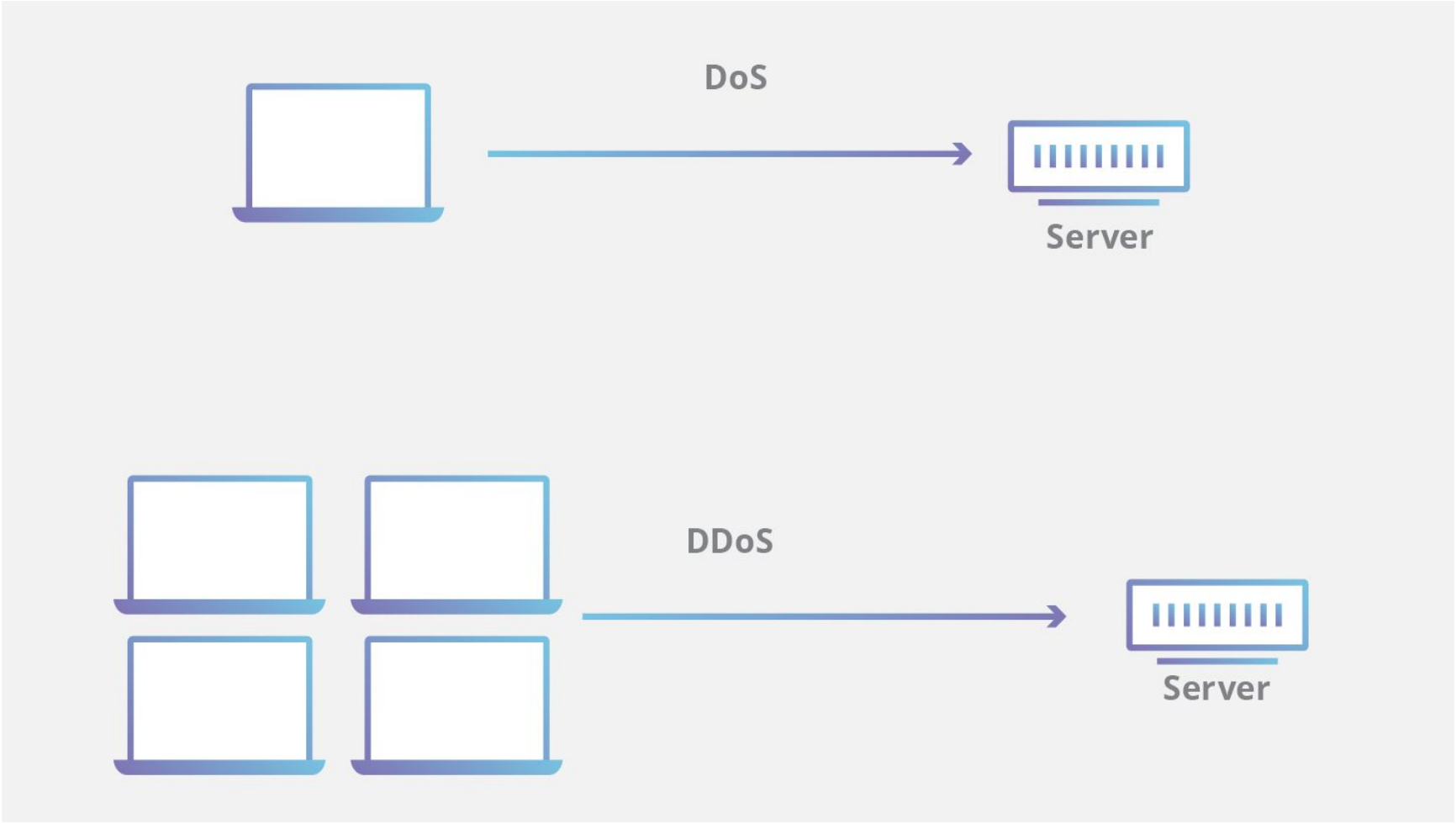
Denial-of-Service (DoS) attack

- Affects the availability of the system and its resources to valid requests.
- Eventually makes the server unavailable
- Causes XDOS (XML Denial-of-Service) attacks.
- An attack meant to shut down a machine or network, making it inaccessible to its intended users.
- Two kinds of DoS attacks:
  1. Protocol Deviation Attack.
  2. Resource Exhaustion.

Distributed Denial of Service (DDoS) Attack

- DoS attack that uses multiple computers or machines to flood a targeted resource.
- Like an unexpected traffic jam clogging up the highway.
- Hackers use phishing emails and a range of other methods to install malware on remote machines.
- Three types of DDoS attacks:
  1. Volumetric attacks
  2. Protocol attacks
  3. Application attacks

DoS vs. DDoS



The Google Attack, 2020

- Phishing attempts against the personal email accounts of the staff campaigners of Biden and Trump
- Iranian attacker Group (APT35) and the Chinese attacker group (APT31)
- The attackers impersonated McAfee and the targets would be asked to install a legitimate version of McAfee anti-virus software from Github.


McAfee
McAfee Total Protection
Protect your digital life and all your devices.
Your trial lets you do all this:
Get automatic updates
Protect all your devices
Get help when you need it
By clicking Agree and using the Software, you accept the License Agreement and our Privacy Notice.
Agree and Install

Prevention

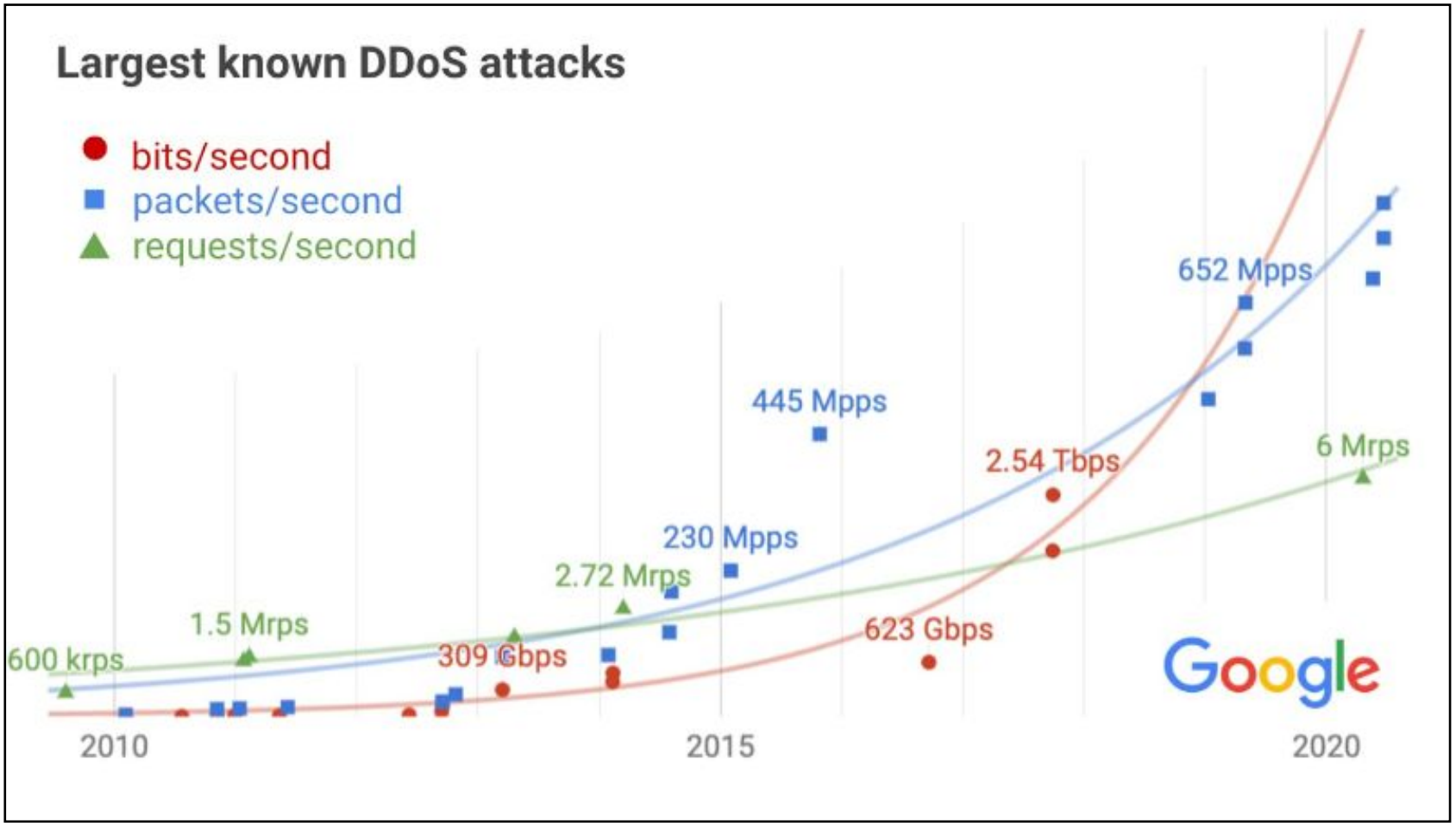
1. Taxonomy of attacker capabilities
2. Trends in DDoS Attack volumes
3. Architecting Defendable Infrastructure
4. Cloud-based Defences
5. Working together for collective security
6. The Intrusion Tolerant Approach

Taxonomy of attacker capabilities

- Rather than focusing on attack methods, Google groups volumetric attacks into a handful of key metrics.
- **BPS** network bits per second is attacking target network links
- **PPS** network packets per second are attacking target network equipment or DNS servers
- **RPS** HTTPS requests per second are attacking target application servers
- This way they can ensure that each system has sufficient capacity to withstand attacks measured by the relevant metrics.

Trends in DDoS Attack volumes

- They determined the capacity needed to withstand the largest DDoS attacks for each key metric.
- Overprovisioning wastes costly resources, while under-provisioning can lead to an outage.
- Plotted the largest attacks seen over the past decade to identify trends.
- Helped them in their decision of what to use for the first data point of each metric.
- After accounting for the expected growth, the results are less concerning, though still problematic.


Largest known DDoS attacks
bits/second
packets/second
requests/second
652 Mpps
445 Mpps
6 Mrps
2.54 Tbps
230 Mpps
2.72 Mrps
1.5 Mrps
600 krps
309 Gbps
623 Gbps
Google
2010
2015
2020

Architecting Defendable Infrastructure

- They now extrapolated to determine the spare capacity needed to withhold the largest attacks likely.
- Created an infrastructure that absorbed a 2.5 Tbps DDoS.
- Attacker used several networks to spoof Mpps to 180,000 exposed CLDAP, DNS, and SNMP servers.
- This was four times larger than the record-breaking 623 Gbps attack from the Mirai botnet.
- Google estimated the expected size of future attacks.

Working together for collective security

- They encouraged everyone to join them in this effort.
- Individual users should ensure their computers and IoT devices are patched and secured.
- Businesses should report criminal activity, ask their network providers to trace the sources of spoofed attack traffic, and share information on attacks with the internet community in a way that doesn't provide timely feedback to the adversary.
- By working together, they said that we can reduce the impact of DDoS attacks

The Intrusion Tolerant Approach

- An active resource monitoring approach is adopted.
- To decide if such anomalous behavior is due to either an attack or a normal operation.
- When a DoS attack is detected, a threshold-based filtering reaction is triggered.

Our Proposed Solution

- The government agencies can ask their staff members not to download software or any application through the Open free Softwares System or by using any links which directs them to download any kind of application.
- Should create a mailing system especially for Professional purposes and not use it for Personal Use.
- Can even use Role-Based Access Control concept.
- Can add multiple login steps to provide more security.
- One-time password(OTP).

Conclusion

- Techniques to deal with attacks predominantly focus on attack detection measures.
- Since web service attacks cannot be completely eliminated, penetration and automation testing should be done as part of every development.
- This will guarantee added protection as well as lower attacks on web services.

Questions?

Thank you.