CNT 5410 - Computer and Network Security: Denial of Service

Professor Patrick Traynor
Fall 2017
Reminders

• Midterm exam on Friday, October 13th.
  ▶ Hmm… let’s take a look at some examples.

• Assignment #3 due on 10/18.
  ▶ Great! You have time to take care of this.
  ▶ Ouch! This is a hard assignment!
"The art of war teaches us to rely not on the likelihood of the enemy's coming, but on our own readiness to receive him; not rely on the chance of his not coming, but rather on the fact that we have made our position unassailable."

-- Sun Tzu, The Art of War
We have covered a huge amount of material thus far:

- Many Textbook Chapters
- 12 Academic Papers
- Research Techniques
- Side conversations, diversions, student questions, headlines...

All these things are fair game.

You are expected to be well versed in the topics we have covered thus far....
Rules

• The test starts precisely at 12:50 and ends at 1:40.
  ▶ If you show up late, you do not get extra time.

• Cell phones are banned.
  ▶ I will keep a clock going in the front for you to see.
  ▶ Too many people cheat, so nobody can have these out.
  ▶ If I see a phone, I will take your exam.

• Write all answers on the test itself!
  ▶ The space is planned to help you with brevity.
Format

- **Short Questions**
  - Should be easy to answer. 2-3 sentences MAX.
  - If you write more, you've missed the point.

- **Long Answer**
  - Questions require in-depth responses.
  - May require math, applying an algorithm, expressing a policy, etc.

- **Applied Knowledge**
  - Asks you to solve a real-world problem with the things you have learned this semester.
Short Questions

• What is the difference between an attack and a compromise?

• Does a MAC provide non-repudiation?

• Why are biometrics considered “fuzzy” authentication mechanisms?
Short Questions

• List three differences between symmetric and asymmetric cryptosystems.

• What is the fundamental vulnerability of DNS?

• What is the difference between Kerberos and Digest Authentication?
Long Answers

• Explain three differences between digest and basic authentication.

• With $k^+ (\{7,33\})$ and $k^- (\{3,33\})$, use RSA to:
  ▶ encrypt the plaintext value 4.
  ▶ decrypt the ciphertext created above.
The recent proliferation of mobile devices has lead many to argue for a resurrection of fully-fledged PKIs. Argue for or against this idea using evidence from our discussion on the topic.
Denial of Service

• Intentional prevention of access to valued resource
  • CPU, memory, disk (system resources), DNS, print queues, NIS (services), Web server, database, media server (applications)
  • This is an attack on availability (fidelity)
  • Note: launching DOS attacks is easy, preventing DOS attacks is hard!
  • Mitigation the path most frequently traveled
  • Two major types: Brute force and semantic
Canonical (common) DOS - Brute Force

- Attack: request flooding
  - Overwhelm some resource with legitimate requests
  - e.g., web-server, phone system

- Note: unintentional flood is called a flash crowd
Example: SMURF Attacks

- This is one of the deadliest and simplest of the DOS attacks (called a naturally amplified attack)
  - Send a large number PING packet networks on the broadcast IP addresses (e.g., 192.168.27.254)
  - Set the source packet IP address to be your victim
  - All hosts will reflexively respond to the ping at your victim
  - ... and it will be crushed under the load.
  - Fraggle: UDP based SMURF - sent to echo port (7)
Example: DNS Amplification

- DNS Requests are small, but responses are large.
  - The above attack is a 70:1 ratio.
- Ok, so an attacker might be able to send a few Mbps… is this really a problem?
Semantic DoS

• Taking advantage of an “artificial” limitation to deny service.
  ‣ “Ping of Death”
  ‣ “Land” Attacks
  ‣ SYN-floods
  ‣ FIN-floods

• Fixes tend to be much more specific to the attack.
  ‣ e.g., offloading state to client, memory management, better randomness, etc
Distributed denial of service

• DDOS: Network oriented attacks aimed at preventing access to network, host or service
  • Saturate the target’s network with traffic
  • Consume all network resources (e.g., SYN)
  • Overload a service with requests
    • Use “expensive” requests (e.g., “sign this data”)
  • Can be extremely costly (e.g., Amazon)
• Result: service/host/network is unavailable
• Frequently distributed via other attack

• Note: IP is often hidden (spoofed)
The canonical DDOS attack
Why DDOS

• What would motivate someone DDOS?
  ▶ An axe to grind …
  ▶ Curiosity (script kiddies) …
  ▶ Blackmail
  ▶ Information warfare …

• Internet is an open system …
  ▶ Packets not authenticated, probably can’t be
    • Would not solve the problem just move it (firewall)
  ▶ Too many end-points can be remote controlled
Why is DDOS possible? (cont.)

- Interdependence - services dependent on each other
  - E.g., Web depends on TCP and DNS, which depends on routing and congestion control, …

- Limited resources (or rather resource imbalances)
  - Many times it takes few resources on the client side to consume lots of resources on the server side
  - E.g., SYN packets consume lots of internal resources

- You tell me .. (as said by Mirkovic et al.)
  - Intelligence and resources not co-located
  - No accountability
  - Control is distributed
DDOS and the E2E argument

• E2E (very simplified version): We should design the network such that all the intelligence is at the *edges*.
  ▶ So that the network can be more robust and scalable
  ▶ Many think is the main reason why the Internet works

• Downside:
  ▶ Also, no real ability to police the traffic/content
  ▶ So, many security solutions break this E2E by cracking open packets (e.g., application level firewalls)
  ▶ DDOS is real because of this …
Q: An easy fix?

- How do you solve distributed denial of service?
Simple DDOS Mitigation

- Ingress/Egress Filtering
  - Helps spoofed sources, not much else

- Better Security
  - Limit availability of zombies, not feasible
  - Prevent compromise, viruses, …

- Quality of Service Guarantees (QOS)
  - Pre- or dynamically allocate bandwidth
  - E.g., diffserv, RSVP
  - Helps where such things are available …

- Content replication
  - E.g., CDNs
  - Useful for static content
Reverse-Turing Tests

• *Turing test*: measures whether a human can tell the difference between a human or computer (AI)

• *Reverse Turning tests*: measures whether a user on the internet is a person, a bot, whatever?

• **CAPTCHA** - *C*ompletely *A*utomated *P*ublic *T*uring test to tell *C*omputers and *H*umans *A*part
  - contorted image humans can read, computers can’t
  - image processing pressing SOA, making these harder

• Note: often used not just for DOS prevention, but for protecting “free” services (email accounts)
CAPTCHA Limitations

• Lots of varieties have been proposed.
  ▶ Text, Audio, Video, and cats…
  ▶ Only a small number have been adopted, largely due to usability purposes.

• Automated techniques to solve virtually all of these defenses…
  ▶ … and people willing to pay/trick others to solve them…
DOS Prevention - Puzzles

- Make the solver present evidence of “work” done
  - If work is proven, then process request
  - Note: only useful if request processing significantly more work than
- Puzzle design
  - Must be hard to solve
  - Easy to Verify
- Canonical Example
  - Puzzle: given all but $k$-bits of $r$ and $h(r)$, where $h$ is a cryptographic hash function
  - Solution: Invert $h(r)$
  - Q: Assume you are given all but 20 bits, how hard would it be to solve the puzzle?

Can You Find The Answer?

$+ \quad + \quad = 24$

$- \quad = 6$

$= {?}$
Pushback

- Initially, detect the DDOS
  - Use local algorithm, ID-esque processing
  - Flag the sources/types/links of DDOS traffic
- Pushback on upstream routers
  - Contact upstream routers using PB protocol
  - Indicate some filtering rules (based on observed)
- Repeat as necessary towards sources
  - Eventually, all (enough) sources will be filtered
- Q: What is the limitation here?
Traceback

• Routers forward packet data to source
  ▶ Include packets and previous hop …
  ▶ At low frequency (1/20,000) …
• Targets reconstruct path to source (IP unreliable)
  ▶ Use per-hop data to look at
  ▶ Statistics say that the path will be exposed
• Enact standard
  ▶ Add filters at routers along the path
Overlays

- Traffic is not delivered to a host...
  - It must pass through an overlay network first.

- Getting into the overlay is where the “magic” happens.
  - What does “Portcullis” do?
  - What else could be done?
Network Isolation: VPNs

- Idea: I want to create a collection of hosts that operate in a coordinated way
  - E.g., a virtual security perimeter over physical network
  - Hosts work as if they are isolated from malicious hosts

- Solution: Virtual Private Networks
  - Create virtual network topology over physical network
  - Use communications security protocol suites to secure virtual links “tunneling”
  - Manage networks as if they are physically separate
  - Hosts can route traffic to regular networks (split-tunneling)
VPN Example: RW/Telecommuter

Internet

LAN
VPN Example: Hub and Spoke
VPN Example: Mesh

Internet

LAN
VPNs/Overlays - Limitations

• Traffic not able to enter the VPN can not overload weakly provisioned end points.
  ▶ Great... mission accomplished?

• Modern DDoS attacks are hundreds of Gbps in volume.
  ▶ Good luck stopping that anywhere near the endpoints.
  ▶ Accordingly, this approach has somewhat limited value.
None of the “protocol oriented” solutions have really seen any adoption

- too many untrusting, ill-informed, mutually suspicious parties must play together well (hint: human nature)
- “solutions” have many remaining challenges

Real Solution

- Large ISP police there ingress/egress points very carefully
- Watch for DDOS attacks and filter appropriately
  - e.g., BGP (routing) tricks, blacklisting, whitelisting
- Products that coordinate view from many points in the network to identify upswings in traffic to specific prefixes.