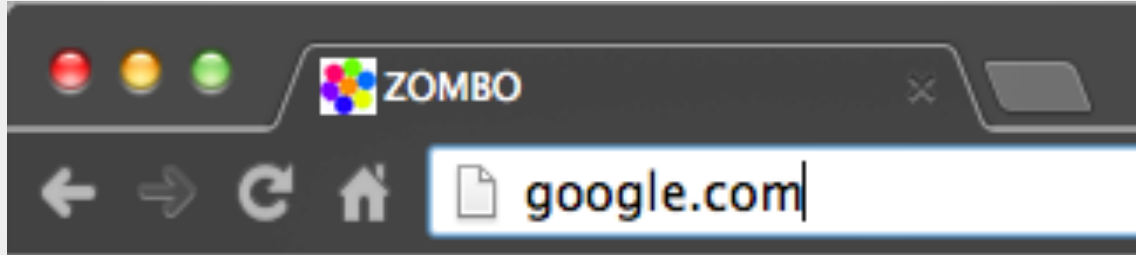


Internet I

DNS Lookup and Information Transfer

DNS Lookup



What happens when we type an address into the URL bar?

DNS (Domain Name System)

Turn www.google.com into 74.125.239.113

- <https://www.youtube.com/watch?v=BCjUbplzRs8>
- Like an address, DNS “zooms in” by analyzing parts of the URL before others
 - Before sending a package to the correct address, packages are first sent to the correct city
- What are the steps?
 - Send request to “.” root DNS server
 - Send request to returned “.com” DNS server
 - Send request to returned “google.com” DNS server
 - This issues the location of “www.google.com” as 74.125.239.113
 - Save address and continue communication with the correct ip

DNS

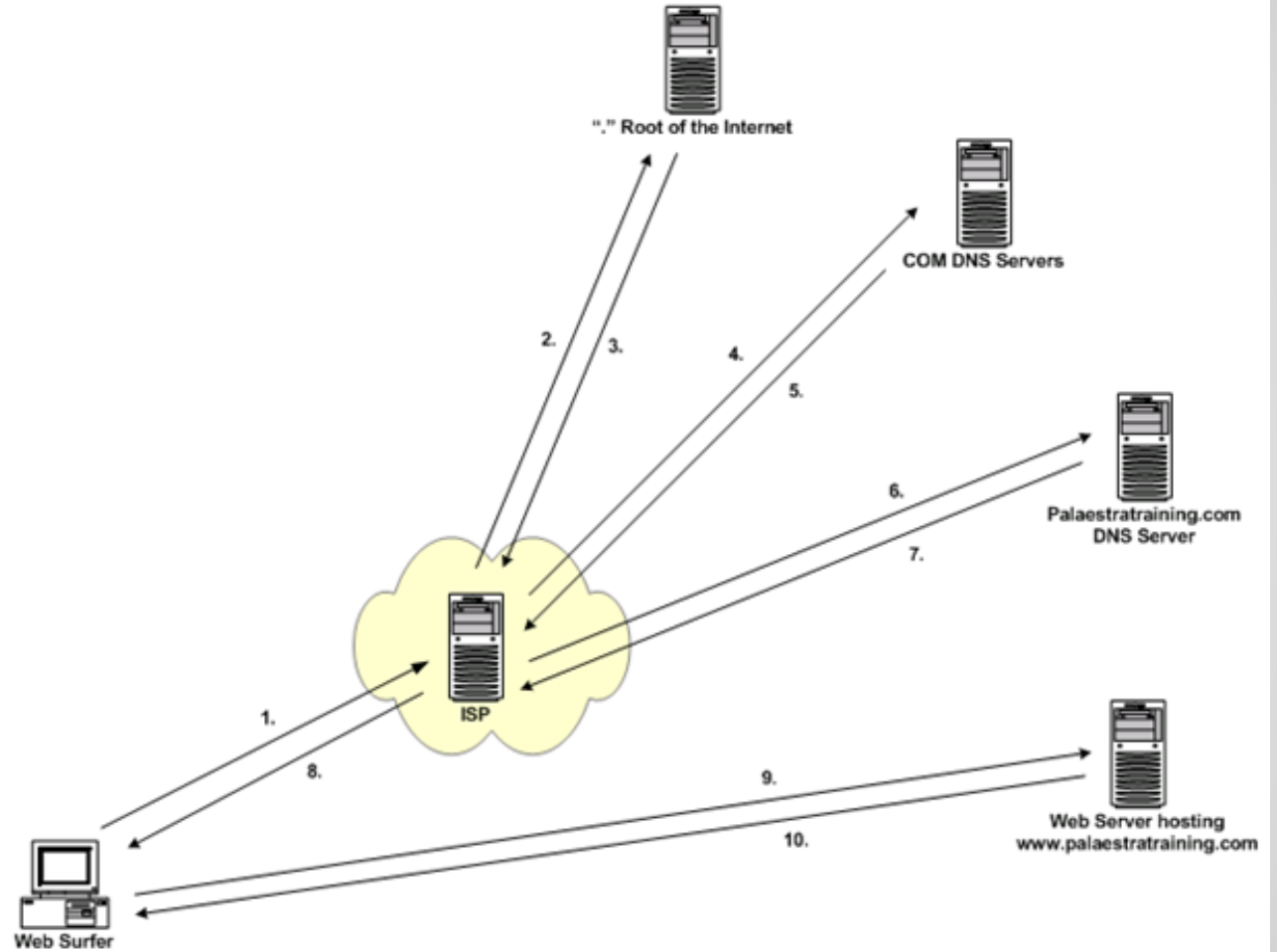


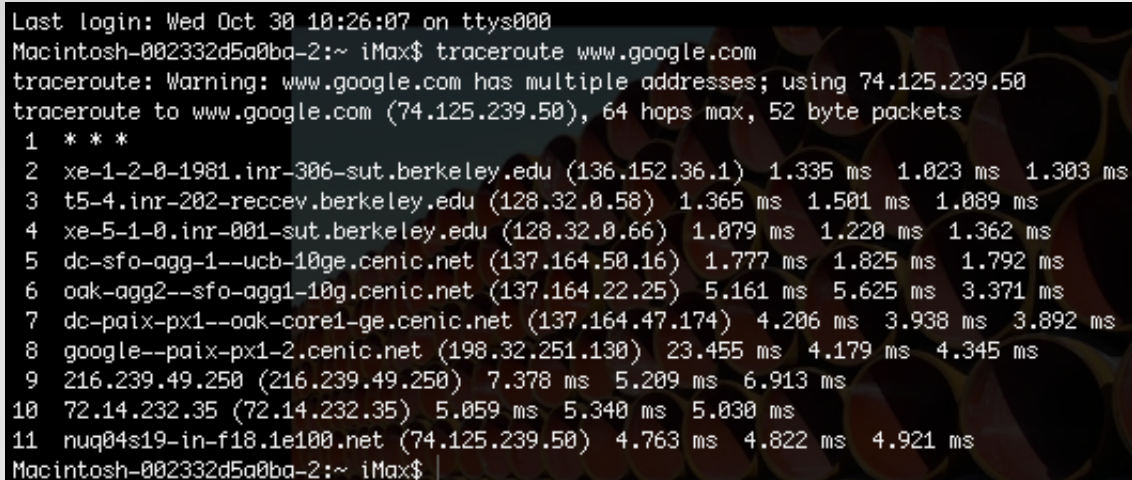
Photo Credit:
www.palaestratraining.com

Question: What kind of vulnerabilities can you see with this system?

Question: What can we do to prevent such an attack?

Information Transfer

How does Alice send a message to Bob over the internet?



```
Last login: Wed Oct 30 10:26:07 on ttys000
Macintosh-002332d5a0ba-2:~ iMax$ traceroute www.google.com
traceroute: Warning: www.google.com has multiple addresses; using 74.125.239.50
traceroute to www.google.com (74.125.239.50), 64 hops max, 52 byte packets
 1 * * *
 2 xe-1-2-0-1981.inr-306-sut.berkeley.edu (136.152.36.1)  1.335 ms  1.023 ms  1.303 ms
 3 t5-4.inr-202-reccey.berkeley.edu (128.32.0.58)  1.365 ms  1.501 ms  1.089 ms
 4 xe-5-1-0.inr-001-sut.berkeley.edu (128.32.0.66)  1.079 ms  1.220 ms  1.362 ms
 5 dc-sfo-agg-1--ucb-10ge.cenic.net (137.164.50.16)  1.777 ms  1.825 ms  1.792 ms
 6 oak-agg2--sfo-agg1-10g.cenic.net (137.164.22.25)  5.161 ms  5.625 ms  3.371 ms
 7 dc-paix-px1--oak-core1-ge.cenic.net (137.164.47.174)  4.206 ms  3.938 ms  3.892 ms
 8 google--paix-px1-2.cenic.net (198.32.251.130)  23.455 ms  4.179 ms  4.345 ms
 9 216.239.49.250 (216.239.49.250)  7.378 ms  5.209 ms  6.913 ms
10 72.14.232.35 (72.14.232.35)  5.059 ms  5.340 ms  5.030 ms
11 nuq04s19-in-f18.1e100.net (74.125.239.50)  4.763 ms  4.822 ms  4.921 ms
Macintosh-002332d5a0ba-2:~ iMax$
```

THE INTERNET

A series of tubes.

Traceroute from Lab shows all the computers your information crosses before reaching the designated website “www.google.com”

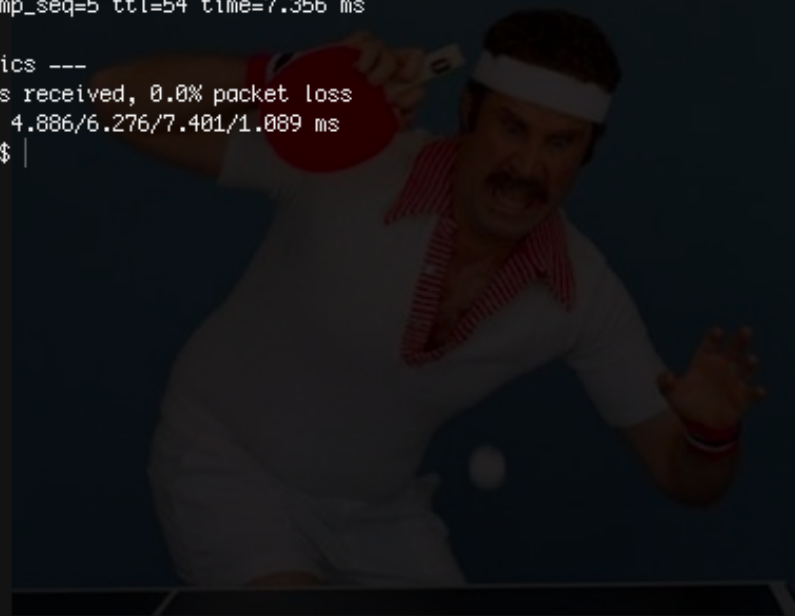
Question: How could more “hops” increase the vulnerability of your communication?

Packets

- Akin to a letter containing an address with “delivery instructions” and some amount of information ~128 bytes total
- Used to carry pieces of your data in discrete packets.
- Statistics:
 - 3MB song file requires about 24000 packets to send!
 - Over 700 billion packets sent every single second worldwide!*

*Based on ~21 Exabytes global data transfer each month

```
Last login: Wed Oct 30 19:20:54 on ttys000
Macintosh-002332d5a0ba-2:~ iMax$ ping www.google.com
PING www.google.com (74.125.239.49): 56 data bytes
64 bytes from 74.125.239.49: icmp_seq=0 ttl=54 time=4.886 ms
64 bytes from 74.125.239.49: icmp_seq=1 ttl=54 time=5.588 ms
64 bytes from 74.125.239.49: icmp_seq=2 ttl=54 time=5.147 ms
64 bytes from 74.125.239.49: icmp_seq=3 ttl=54 time=7.401 ms
64 bytes from 74.125.239.49: icmp_seq=4 ttl=54 time=7.276 ms
64 bytes from 74.125.239.49: icmp_seq=5 ttl=54 time=7.356 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.886/6.276/7.401/1.089 ms
Macintosh-002332d5a0ba-2:~ iMax$ |
```



From lab, Ping times how long it takes to send and receive a packet from a website.

Delays

- Packets are fast
- But not instantaneous
- Delays open window for sneaky attacks
- Packet delays limit how much information can be transferred
- Question: Can this delay compromise...
 - Reliability?
 - Confidentiality?
 - Integrity?
 - Authenticity?

