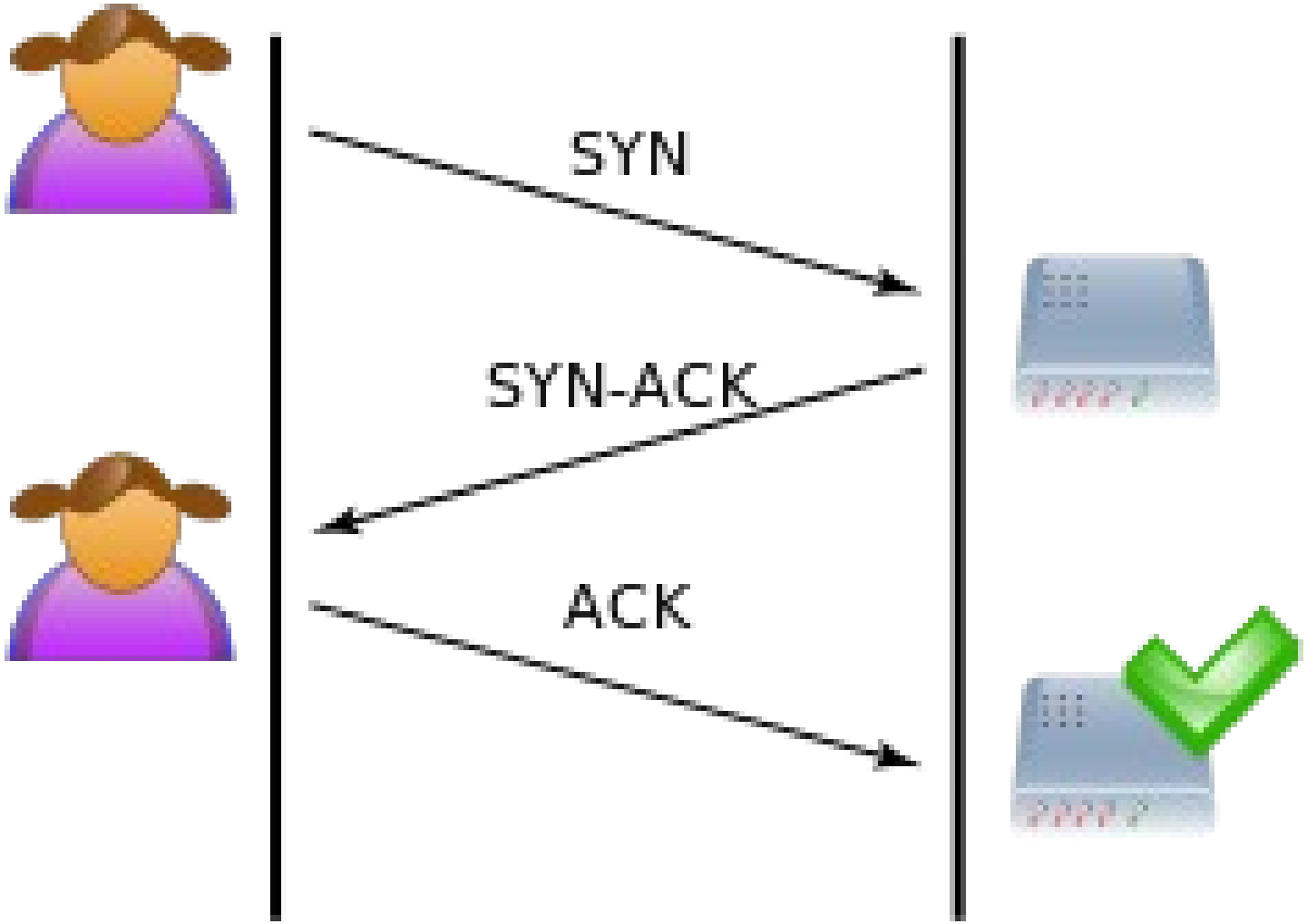
DDOS – The Basics

Distributed **D**enial of **S**ervice

- Distributed – many network endpoints send traffic at once
- Denial of Service – prevent users from accessing your service
- Typical forms
  - Volumetric
  - Application Layer
  - Low-rate
- Other attributes
  - Reflective
  - Amplification
- Unintentional

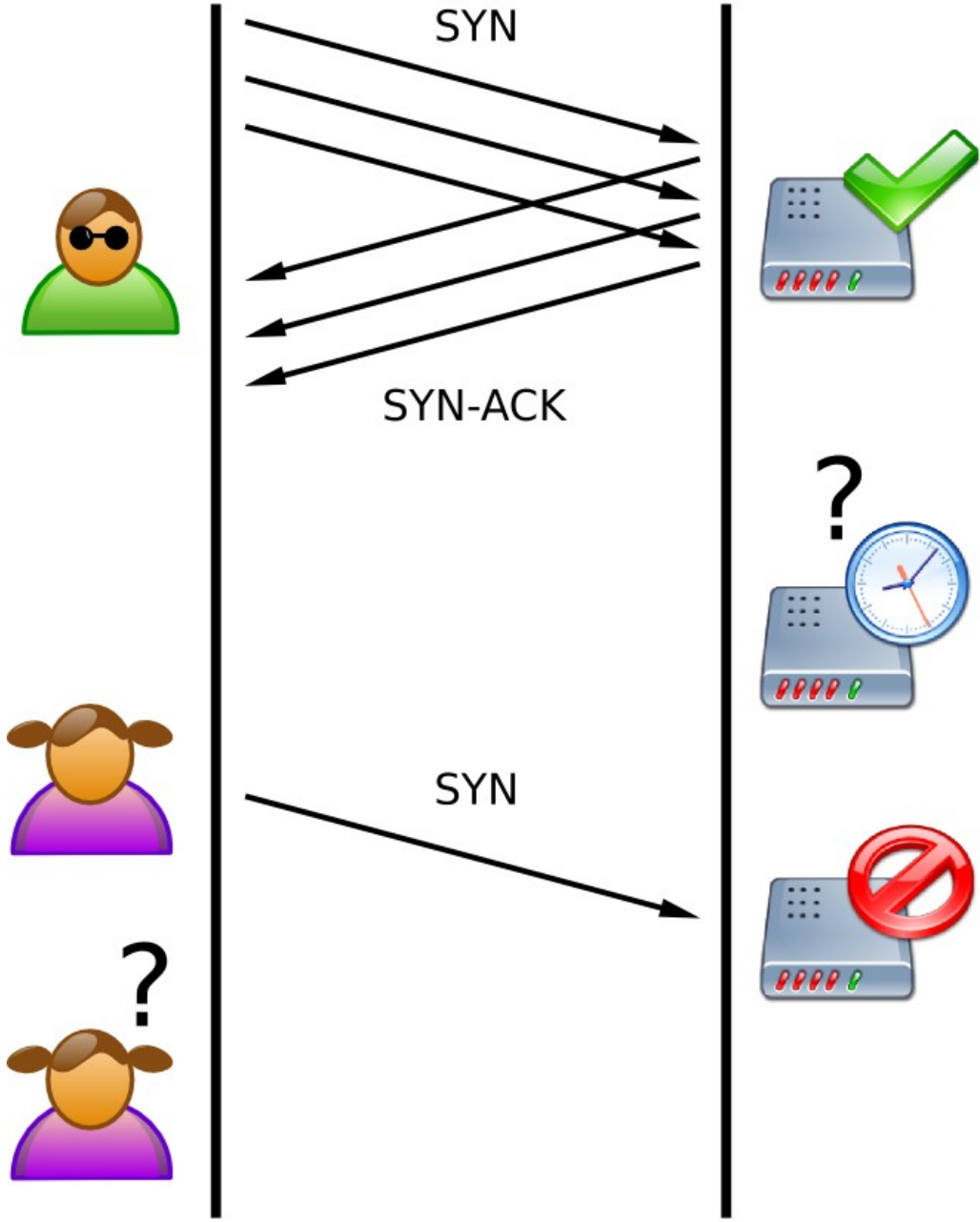
Normal TCP Handshake



https://en.wikipedia.org/wiki/SYN_flood

Syn Flood

- Attacker sends SYNs without ACKing
- Server holds open those sockets, waiting
- No sockets for anyone else = no service



https://en.wikipedia.org/wiki/SYN_floo

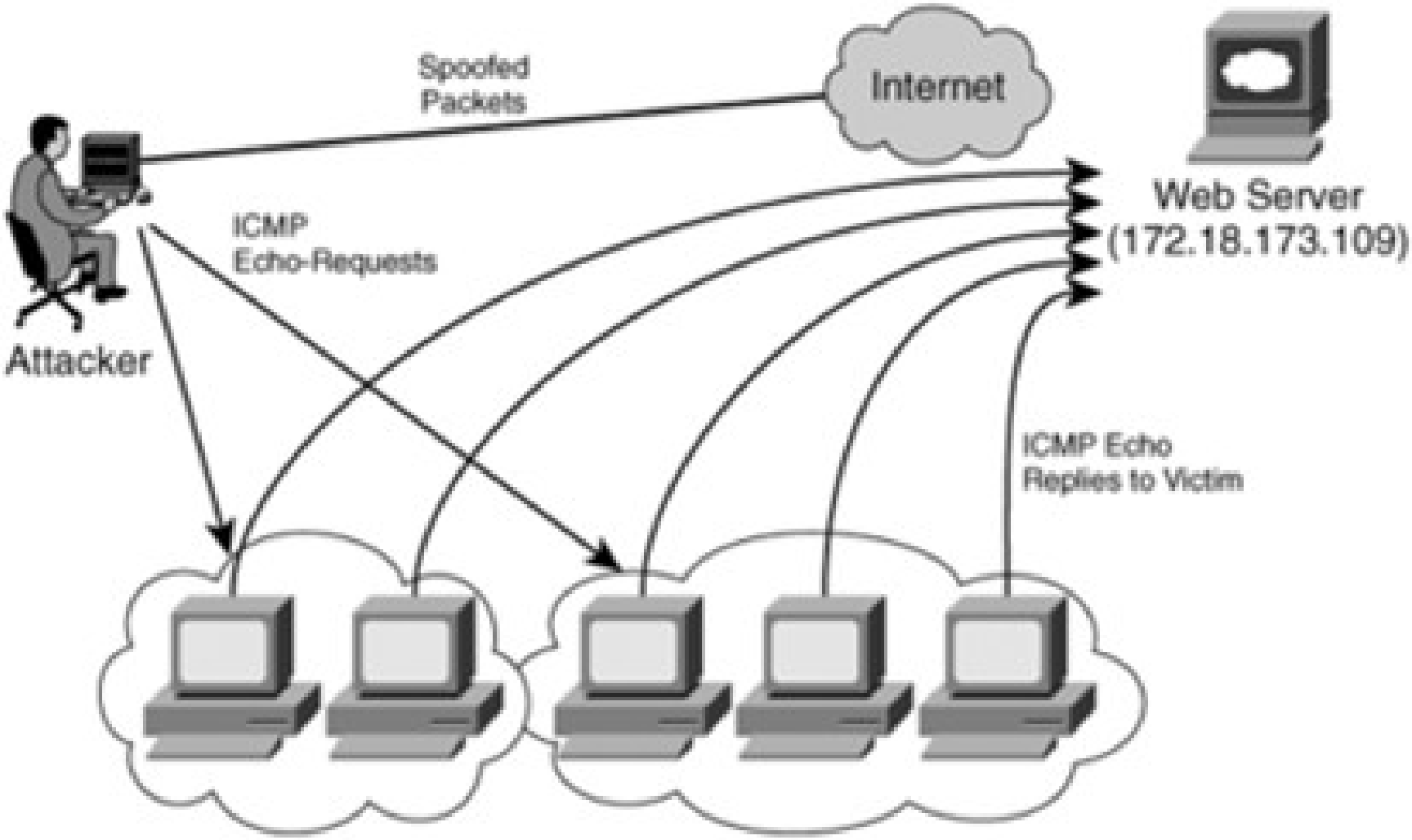
Volumetric

- Make the host route, parse, filter excess traffic
- Or, Clog the network links
  - Imagine a series of tubes...
- Protocol is largely unimportant
- Ex. TCP SYN, UDP Flood, ICMP Flood
- Collateral damage
- Defense
  - Filter ports at firewall
  - Filter invalid sessions
  - As far upstream as you can to lessen impact

Reflective

- Bounces traffic off other servers to hide origin
- How?
  - A little about UDP…
- Ex. Chargen, Echo,DNS, NTP, SSDP, Source Engine
  - Basically any UDP protocol.
- Conflict – provide open services vs. prevent abuse for DDoS

Reflective example



http://resources.infosecinstitute.com/the-red-spike-ddos-mitigation-strategies/

Amplification

- Sub-type of reflected (typically)
- Small traffic from attacker → big response from reflecting server
- Ex. DNS TXT, DNSSEC, NTP Monlist

Amplification

Question: “ANY cpsc.gov +bufsize=65535 @8.8.8.8”
Response: 4016 bytes!

;; ANSWER SECTION:

cpsc.gov. 810 IN SOA auth00.ns.uu.net. hostmaster.uu.net. 994777 1800 600 1728000 21600

cpsc.gov. 810 IN RRSIG NSEC3PARAM 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. SdIIiFyGbv4jx/N9+7M8QxT+PZ0rz1ZBpcUo4ZSEBv5aU1HgOr/MTZnw pNjlbXb8w3s3uOwudAZxMIp0ULZeySrSQDNfRdY5khgeDk/q3p/m7y3E i3d2/zVepslGKQCUU845H9k/GsGC44dSdR2Ob1IYI+cvWRteUVDreAVH 9F9ItxcGtRQ7rNM5QsMVfBp1GeDrpX9+AauOLdNR2nnv0FecxPU+8YDi rzLS9WhQnSeU2DyYJNwDhifiifjURTTtXSxcm9JBH+migELHauxAqqp9 KAGdgaNZSo8QeWx9mf7IE8WYw5b/6NI9/hU0cc1zh7ifuxrceRiNhPBT TWNuLQ==

cpsc.gov. 810 IN RRSIG DNSKEY 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. sSFRRwZkti0eP+/5UU8GCwmB5vhQT0R7mpS1uiE16wIIWwwqWX9+Dh78 6al64n7ZM899AzuFZ13v2mcNcUBtrPbRlJmwAXvF8eVLhA2I1HxHCgts rzcqbhdGAMhl2zJ8Ki4KX4VmBaafxixgilKzESnL06NKLpEzWA5WjV+T KFIaqGkovpjI7dVqEEaizDjStEV2zSAB2XC6GAbHPKb66dR0bcAbjlnq rNaI+P0dcFv0hgXMB0MR8G+KVtd0hMwGciO/vVeAEWgzhyDp2dHDiJk7 XQ+c3+nyIfLUlkJ1Y748zCg4J/OAqjDQi+auYKhxHpkprndYvhEf0xcK D4Q+2Q==

cpsc.gov. 810 IN RRSIG DNSKEY 7 2 21600 20161109030505 20161102020505 58273 cpsc.gov. XRKhQgW251w88SEO4WukuiIea6gaGSRHYbmjzTLLZtBLxqjk+WH1MhEk ZMFoYhfc+gTj6Qm/EIw1yjzXJoPrapdwVhEvizj5kZnoXYvKG8OtlAkk LuIzPrpXx3dEIVMSlV0koEeJT2efwvWM2U5vub6QijiPaKjrzaPvxms0 Ki/9kR5TktynidkZwPNSdkyGOWG51RIlb5K55X+a0FBZBEYQIDfpNSi+ uPkKnpK/H8b5BeYpxLuU7T7lYe/2N5rsIIPZNbESP0MMWMHC9eU50fUi bPjUBAwl+z6fwxg22+wnTxzy9UjRyq7lH5bn8SLvhCTqyMX4xqFZOZ7h JuN1qg==

cpsc.gov. 810 IN RRSIG SOA 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. YcYizrWRjaXG2xrIsC0Q+tLn7Af7V1rl5Cs617kI19HMITqpGYN1Nnhl HQEmhMVV5bo2IIewM6pp4y6hUkQfa9VeZqKGjeJsng1WKN2WOrkZuQ/s R9gymylpv7qdJYkt1BzgrY/X6Y9p2BJsngjMkGLOpStlfF+H93ilkdMr j/PcHIfGx+qrTMUtRHnyEsIe1WCm2kSgiQO4uqfNX6GNRNraPkTOLxWP 3xzTf2VjVN/E2lK+c2ZU72Ga15lOU5xvvQi9MjWKAxYqgoqZByo58+DY +iZkH2/+4J2+Nm5A4UceFXjIXL1dn68AeXA75IBG9xqtxT0isI1IryZe XnYNGg==

cpsc.gov. 810 IN RRSIG AAAA 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. ShNKZG0YV3MCpkOiddZFviNIQqPV59abgzOCLp3ktsCZA/IULvjYX1dW JNS16xQFrS1b7O7FZyAQi2oc4RvuenfQgst9cztn4dy/eH6XIdLqF7+Z xH/H2PTR3jsh7e1ax9AKHG6s/BhH+EXmb126/SQL34HrdgTS8fY6taVM nxRCwtxhWvl1nF3qquNVk/GEbhDlleC/pJgWh2L4L8PqPOKetosXflpk urFxL174tiVURJ+VXBKmb8694vAE5YrPknbDFjtTI9kM7kBeD5JUDzrL u0lSIpL2sn0jHndnF9/t8KEcdODbLGGT5JaxxOpYg2ZuaAyJJFZRApeJ tX1F4Q==

cpsc.gov. 810 IN RRSIG A 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. spX2HucXx7ZjuA1zazIvQnM+QM6onWGSzs5lc+uNxtf/UaXzxdV3f3Gj cMF81wMg0kPCRni9PQX0VZq/I7Ig73/VzLvHRcTj3BGqrfe4isYBeEdF JJJdkYlcqKuSoRWkZV9sDNOvbhi+RFGQFlcLExqMOm2JtQh2lutlfdG4 XJ2o8RaXS9pGq11Q9pVJkpcSyN1YlyQZVeMFprhI8oREhZJ76424kcvR Fz2E3O9iqaWgU1RtBuebzqqXWUx221cV7OIJwVFC8yy5XZs4/6s+K4vt YVc4gLh+McBRjo4E2H6YfUxF7Shjsz6G3h22Bod/xlTWicUNnbSLowzI bRTpqw==

cpsc.gov. 810 IN RRSIG TXT 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. Dkm9AKOPesQ1eI8dnF6tzqhUsEfnCCV5eWLKOyRx+Lk/AEKY/FpXTAro wJET32aQ8VU7jc4hf5u/ScuVKQtyUvd5vm8HagktB6Csu+dSGhEt1F80 vsX2nnXXj43ticg9rQxDesOylPsdVnEzOjTivU73SQG3edd02MfSfV1M v3+cX65oEMA5/9a8Dy5oegQACXntzjX+7pU1GS43gNibZErscnpbMhQq YeIRbMeSTXZm7PheWHSHRFqF56SFVEwSbIKMszHjhT+60RCO2LKlsz5y HTCflUJ58uuHea/yuhPD2r8WKQ9SbCkpYuM0wHslGft62s10FaxMqbG4 +w+VvQ==

cpsc.gov. 810 IN RRSIG MX 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. wnWcCMQeGkcQhBAHcQTcEnBxRcbF8M4PkEO/FMa8cR9IJhxHzviAX3fd vteGMf2mfBIYEgs9Fzbv6eiGNVsznsCLhuy6Jx1e/V+vQs/4jF77fD7N 0O+2A7gJ2yl2qN8RGbatJ2bvEtRc+9m7Nq5VbycRrVTqiUxLpexXRpj2 8h6Z57SjvmxMSJTbJcGDzb58yAdW1dD8XI/U8bh/D4ZrLFIyyADwf0Hh frWzqZbiYYUW7m2Zt6+6GOQfc784Z2M1JTCECFP0iPRM1XA2GvXXrgrI 0KD/Iiyn4YpOCy+xpmDsUkLHPZapMX/Q00+COMk8yBtyxxTRV7ERZYMz qt9fRg==

cpsc.gov. 810 IN RRSIG NS 7 2 21600 20161109030505 20161102020505 11142 cpsc.gov. Cbz7x9vI4IyH3zOXY+QlU+ch2qFy7WYBT5BBzIkXWIYVQba/EM9CZBVT mgp/1KIn2BWhETtSUVzXgMmzjr2/AQxmdg4aZM/G47ZvEyi2ircEbuUm 130wPKiPB8SLlu5Gd0NuvOvs7Bwt+WubaEi5XR/ic4tqE6J8kVgkKI+8 mwEBy898kTFtMuaSRl/xru4pOR1jKTLtAm5DsP7xjhqB12l8C5alqXy4 T8STH4xSjObHpnIHHgcnf42T0uQuy2lJZr0CInpHBMgcLmNtz0m0yciY ZX79l7BMmJlwMVOMA1kDXuPcwKNPA7jCjxZFwEFe7jg+ft4slqS7hEQg 5o0OWw==

cpsc.gov. 810 IN NSEC3PARAM 1 0 12 AABBCCDD

cpsc.gov. 810 IN DNSKEY 257 3 7 AwEAAX5Tor9V7TnhfUMAL67reT+IFYd+4ciQv/UnvZbNgj7DgDuJPpcl Owh6ypAldCYgTXkF2Qt+an9WVp+Khsp2wRCCOhvGIUR9sOGdzxumDUCT Uru2dxHAqIn1QYSjuT8huMDDyBJmnoA4AY1Te86mcE1Jwpo+S9KoB23Z JgnMedU+6i8Qm9cdGLNM7nqEXhgKgmKc/387UFdh25jltsg0d2gOK//q k2HfLdDqv8XlrlacfMsSXniVwK7E6mtqcfbF518M2bl6UFJWXuxp+cU8 0WdmGiQfxmLvm62a2aVs9IzR6qGg0Ce5bxbx68v6gYTgIOUBm8ERytZ3 T2jzc0QOKQc=

cpsc.gov. 810 IN DNSKEY 256 3 7 AwEAAepXgcviRvTWTMcZ4MjFlZe/plj2y6gkDQf0GTgc3mb/UznTvAsu 2ABKSTLxKSLSsVXfSXVBwSSHS3d91My1B8QUf9Z2Uq0PpDR91ALH6KHm apiDwI+IBDIlzT2XNC7QYaqHp8JvxeOLUf2i/PWIB5w7NlYHbt0NF+sg wSPm34eTpqRDQUCKp3DwmlzTwnb54Wk2wQC3ZosFZtJZ5H+LaRjTbS3k y6GPY0wB6C+2z27fiR0rtPd3uGNQKIVu0qrUatZAj4Lr6HE9CkD8PVQF 7QC+k+/MdoKVmKRyX3SL6TJBq5PbgMS/VOJEmYwx/4aXBADd4Bk1YW+u Ijl84w4DB5s=

cpsc.gov. 810 IN DNSKEY 256 3 7 AwEAAaUVm4E/3J5ew8NovcTallAv4Zrtsy7nJuTFzZsXMHnSYdWIIHwp LheuElljnOUZsacX4VkZoLRrJyzVortC6AlXVfUNtJSUxREkGzFRHBvD gC3fqe2Qk9MDJGoMasNbJkmuk+RvvMSE460CTGLg38E7QjI7fHHHg8Fd ywP7mNqNVs44a8uDdpAsUDkDkWh4khK3EptLyedpj/LxCeTWeotgA08P cDsD7ICguuHqqjGdrwugC72YLIxDeJcduXdWy2xo02NNmnUmiXcNZenG GkUjt3gl5+KURHyPnqBKKLBTArQhAT9NeUXLY5VaWgxBMw1JH0yybv6J mPTfmMPj990=

cpsc.gov. 810 IN DNSKEY 257 3 7 AwEAAZztz17cVspxUk8egfYEFLuyPXVETlPdT2PAuy+cZTk3afTS7cda Tnsk43AlqgnCkTvHE9m4gVuOhNmFjPlABPkfmaCtOzyqVmLjxb36JMxJ TnhBPBYjWY0HrBdEGCGG7eZzY4ll9kAMPlxE1OmMl9iM0dQSzamITEWN 89oPptHnlbjz8k7nQO3xyzXreamjhIW/2iIJhM+CdHe2CgMhPtf8b4QR 8CuIBMH07gvsTKljuvQLiS1ThQYYpmLgriiWjnQFum2FJe6J7x8joDAq YCzbQUdGSyJPp6FYibaG70Y62fIf9DNgHRMH/3c79DW9RmwzFggjfKLf y4hOgRbsVFc=

cpsc.gov. 810 IN AAAA 2600:803:240::2

cpsc.gov. 810 IN A 63.74.109.2

cpsc.gov. 810 IN TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.cpsc.gov -all"

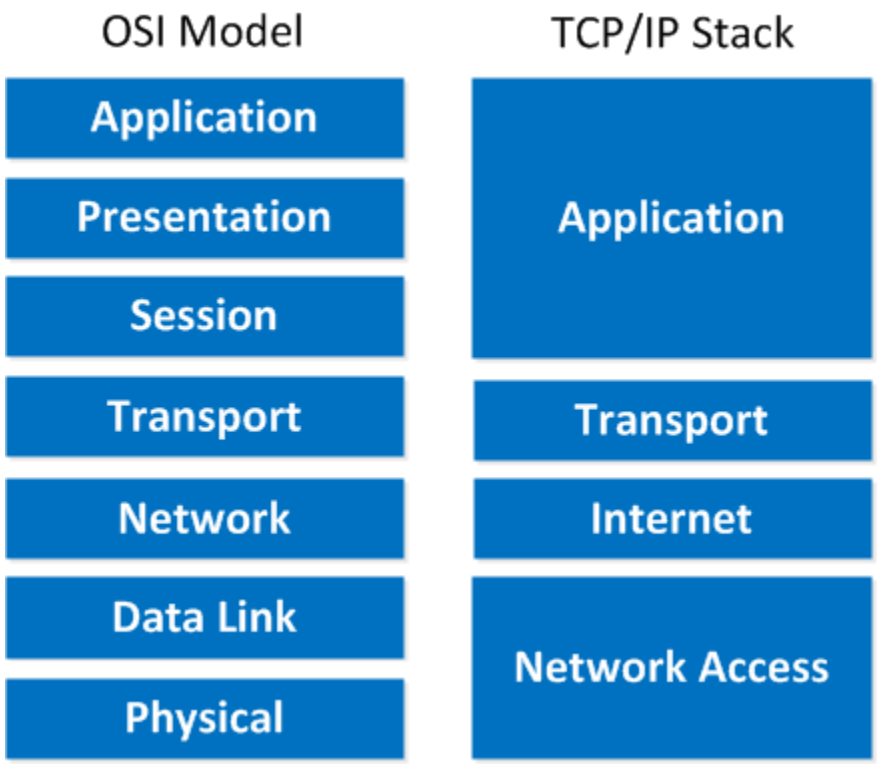
cpsc.gov. 810 IN MX 5 hormel.cpsc.gov.

cpsc.gov. 810 IN MX 5 stagg.cpsc.gov.

cpsc.gov. 810 IN NS auth00.ns.uu.net.

cpsc.gov. 810 IN NS auth61.ns.uu.net.

Application Layer



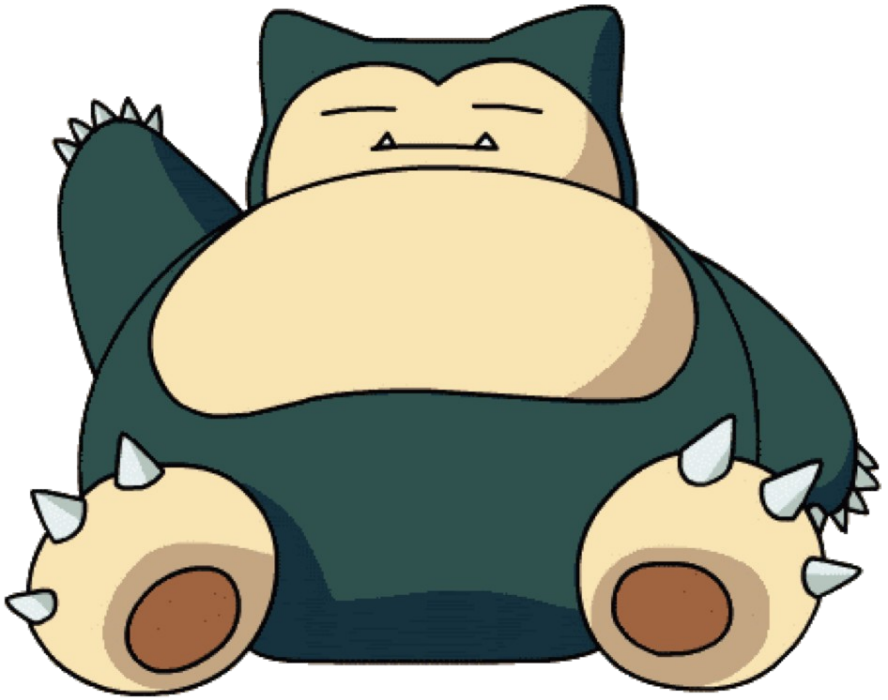
https://cdn.networklessons.com/wp-content/uploads/2013/02/xtcpipstack-vs-osimodel.png.pagespeed.a.ic.Yr-rab7gll.png

Application Layer

- Resource exhaustion
  - Start too many application sessions
  - Use too much memory or disk space
  - Run complicated/heavy actions
    - Site search
    - Large images
- Crash service repeatedly

Low-Rate

- Protocol trickery and state machine dickery
  - Slowloris, RUDY, HTTP POST
    - Tell the server to expect more data and never send it, or tell the server to keep waiting



http://pokemon.wikia.com/wiki/Snorla

Unintentional

- The Reddit/Slashdot/Digg effect
  - Is Digg still a thing?
- Legitimate outages
  - ...and the skids who claim credit

Botnets

- Compromised or paid-for machines w/central C&C
- Often personal machines
- But can be servers
  - Cloud services are cheap + disposable
  - With big pipes!
- Internet of Things devices
- Sometimes even big-iron routers…
- Often multi-function malware – does DDOS and more

Botnet recruiting

1) Scan internet for vulnerable machines
    1) b) Or look in Shodan, Censys, ZoomEye...
2) Infect w/DDoS malware that also scans
3) Wait for instructions

Booters + Stressers

- “Legit” services to “test” “your” website
- Accept cards, Paypal, Bitcoin
- ex. vDos – offered API to other booters to re-sell attack capability (including PoodleCorp)
- Often based on botnets, sometimes on rented servers

Common Targets

- Businesses
- Governments
- Gamers
- Journalists
  - Krebs On Security
- Critical systems
  - Dyn DNS
- And with booters...anyone online

Common Motivations

- Protest + anger
- Punishment
- Turf wars
- Distraction
- Extortion

Extortion

- Pay or your service goes down
  - DD4BC
  - Armada Collective
- Some scams – threats w/no capability

Internet of Things

- Interwhat of huh?
- Formerly “embedded devices”
- Typically low-power, using ARM or MIPS processors
- Includes:
  - Home routers + modems
  - Smart home systems
  - CCTV DVRs
  - Connected cars
  -
  - SCADA/ICS devices*

Internet of Things

- Infectable
  - default Telnet or SSH creds
    - Yes, Telnet.
  - 00’s era web exploits
  - Old versions of Linux + libraries
- Invisible
  - Rarely patched by owners
  - “Wait, my toaster is a computer?”
- Derpy configs
  - Why is my DVR running NTP, to the outside world?
  - Why is SSDP pointed outside the LAN?

Defenses

- Main objective: allow valid traffic, drop attack traffic
- Filter unexpected sources
- Filter unexpected ports (ex.web server=drop inbound DNS)
- Filter by packet size
- Rate limit
- Traffic scrubbing
  - TCP handshake tricks
- Blackhole or drop top talkers
- Also: CDNs (Akamai) and DDOS defense services (Cloudflare, Prolexic, AT&T, etc)

Questions ?

Resources

- http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html
- https://zeltser.com/reasons-for-denial-of-service-attacks/
- https://www.recordedfuture.com/dd4bc-cyber-extortion/
-