Internet Public Health Crisis

Paul Vixie, CEO

Farsight Security

2014-09-15

Ground Hog Day?

- The great challenge is in finding any trend, any change, at all in the last ten years.

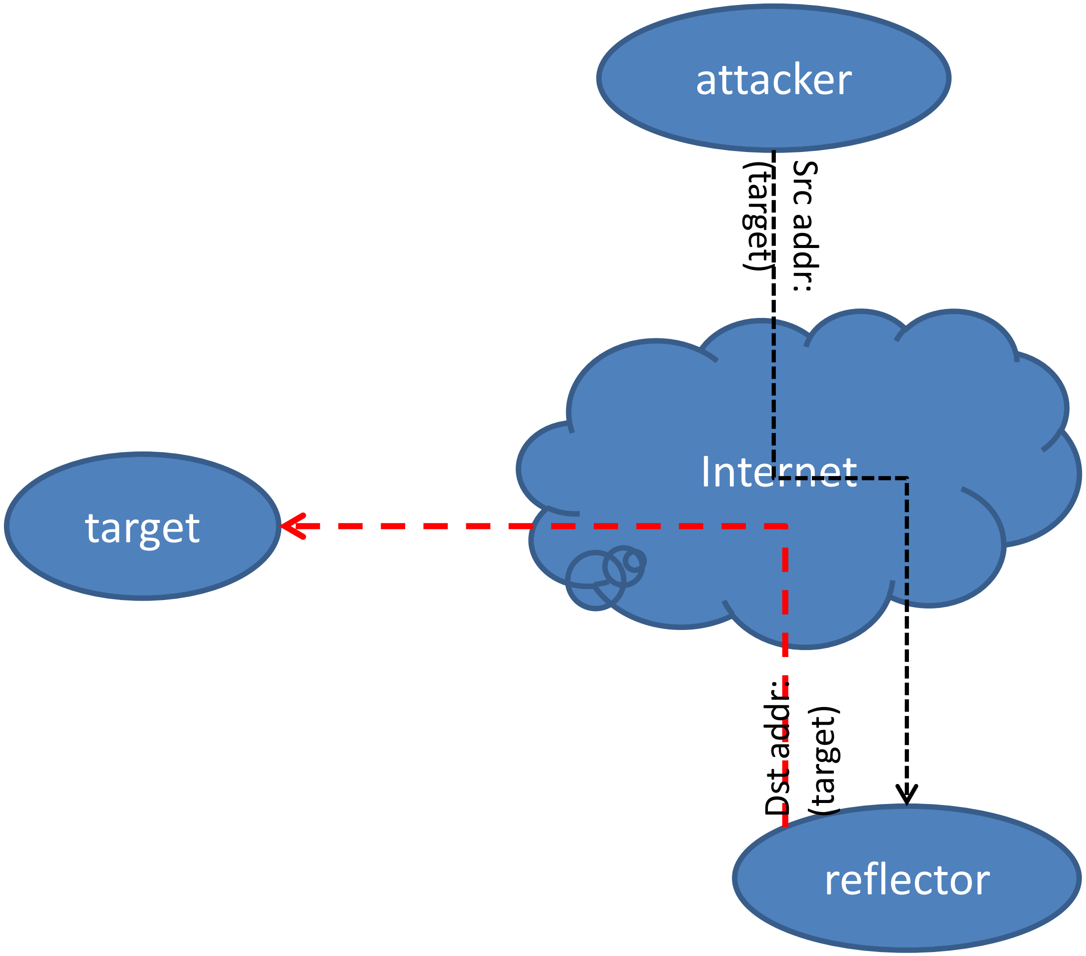
```
Jun  4 03:12:56 ss sshd[64137]: reverse mapping checking
getaddrinfo for hn.kd.ny.adsl [182.118.7.234] failed -
POSSIBLE BREAK-IN ATTEMPT!
Jun  4 03:12:56 ss sshd[64137]: Failed password for root from
182.118.7.234 port 45948 ssh2
Jun  4 03:16:12 ss sshd[64160]: Failed password for root from
116.10.191.172 port 41359 ssh2
Jun  4 03:16:42 ss last message repeated 5 times
```

What’s Our Biggest Problem?

- “The most common attack on Internet hosts or infrastructure at the time of this writing is to cause the receipt of too much traffic, consuming all available resources on a victim's host or Internet connection. This is often called a "Denial of Service" (DoS) attack.”

  (ICANN SSAC SAC004, P. Vixie, October 2002)

Spoofed Source Attacks

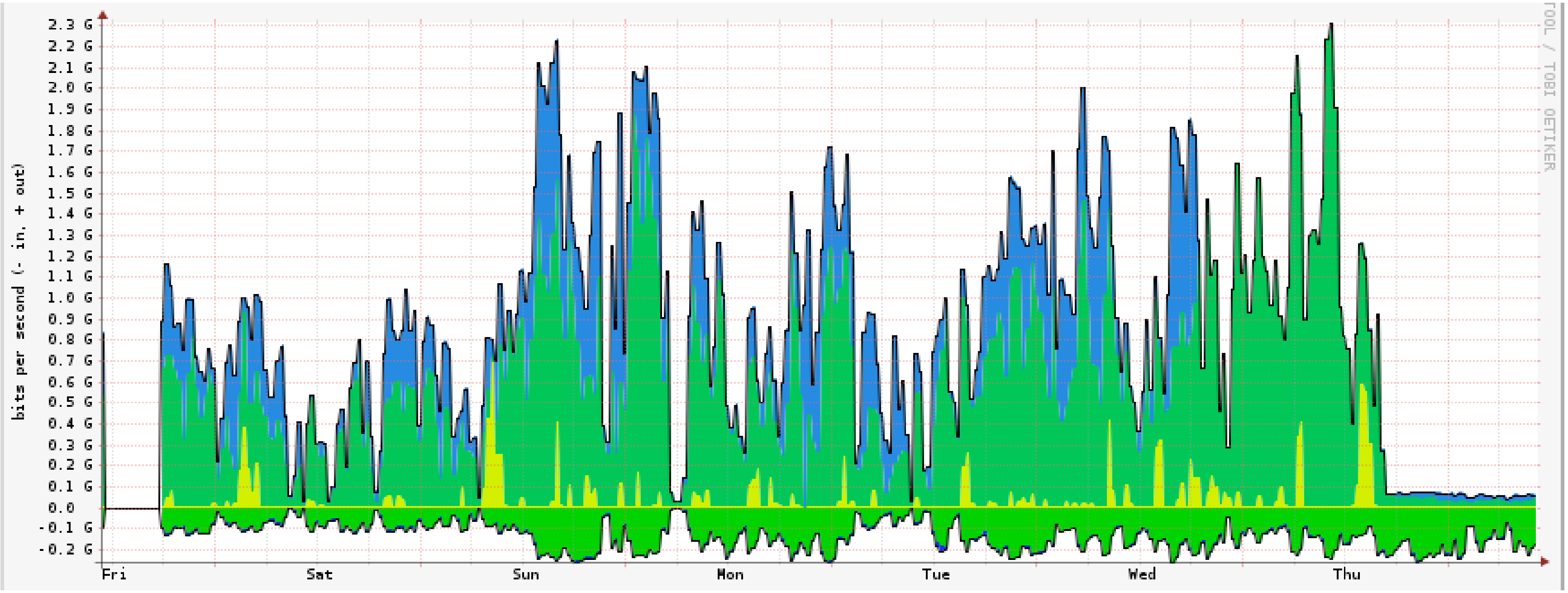


© 2014 Farsight Security, Inc.

Hopeless Trends

- No incentive for up-front security engineering
- No incentive for network output monitoring
- No incentive to share actionable telemetry
- Oft heard complaint:
  - "I'd be making all the investment,
    but my competitors would be getting
    the benefit."
- This is the "chemical polluter" business model

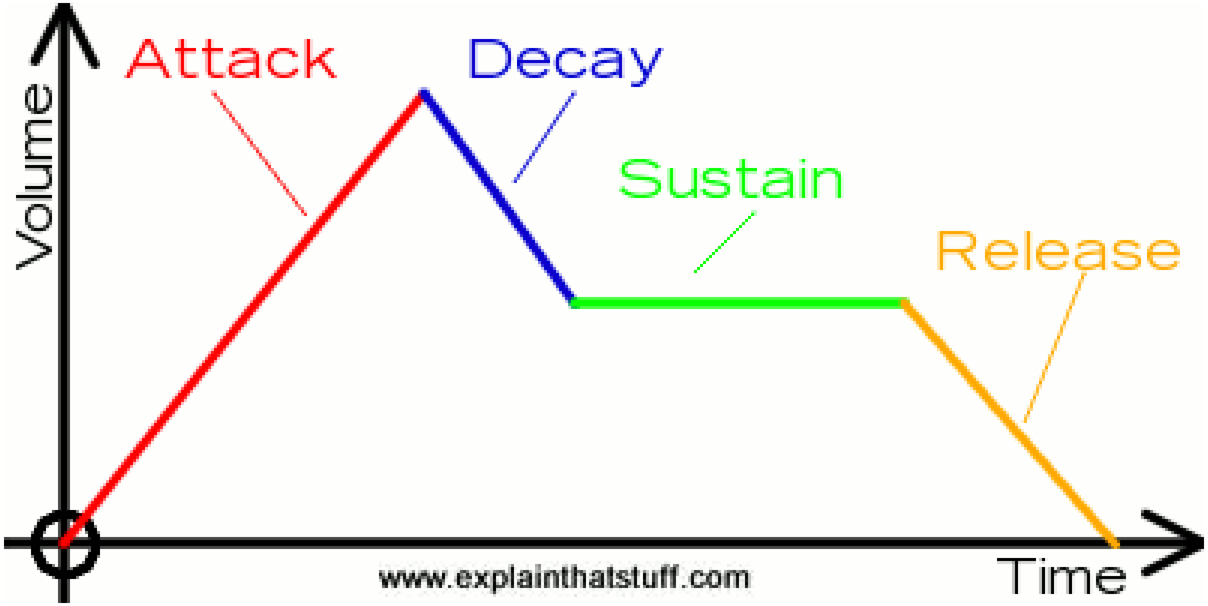
Hopeful Sign: DNS RRL



Value Flows in Tech Economy

- From the tech consumer:
  - – Money spent, to the tech producer
  - – Money stolen, to criminals
  - – More money spent, to security producers (e.g. AV)
  - – Lost privacy, to pretty much everybody
    - Free service → you are the product
- So, we are **all** counting on the tech consumer to live a productive life and bring us their money and their personal information.

Revenue = area under the curve



Product Security Incentives

- Tech producer:
  - Competitors control margin and product lifetime
  - Therefore producer only cares about TTM, volume
- Tech consumer:
  - Only cares about features and maybe cost
- Product security is an afterthought at best
  - E.g., X.509, I-CPE, Windows, Mac/OS, Android, IOS, Flash, ActiveX, and especially Java

Conficker

- MS08-068 was not exploited until disclosure
  - Note previous bug fix
- Turned off antivirus
  - Infected population is still ~1M uniques per day
- USB keyfob vector
  - Autorun can choose “folder” as its icon
- Mitigation
  - Example: hospital

Heartbleed

- OpenSSL bug in plain sight for several years
  - Has open source been out-scaled by complexity?
- Unexploited until after public disclosure
  - Has phased disclosure process been out-scaled?
- Revocation does not work, shouldn’t be done
  - X.509 CA system has never been secure/resilient
- Is scanning good, or is it evil? *Yes!*
  - Example: HP ILoM; see also IPMI

Heartbleed Cleanup Note

- "In addition to patching, many sites replaced their TLS certificates due to the possibility that the private keys could have been leaked. … Even more worryingly, only 10% of the sites that were vulnerable 48 hours after disclosure replaced their certificates within the next month, and of those that did, 14% neglected to change the private key, gaining no protection from certificate replacement."
  – *The Matter of Heartbleed* (IMC'14, November 5–7, 2014, Vancouver, BC, Canada)

Ode to David Isenberg

- *Rise of the Stupid Network,* 1997:
  - "Why the Intelligent Network was once a good idea, but isn't anymore. One telephone company nerd's odd perspective on the changing value proposition"
- David was right. We needed to innovate at the edge, and the core had to be assumption-free.
- So, the core is stupid – like it has to be
  - But, so is the edge, which it <u>must not</u> be

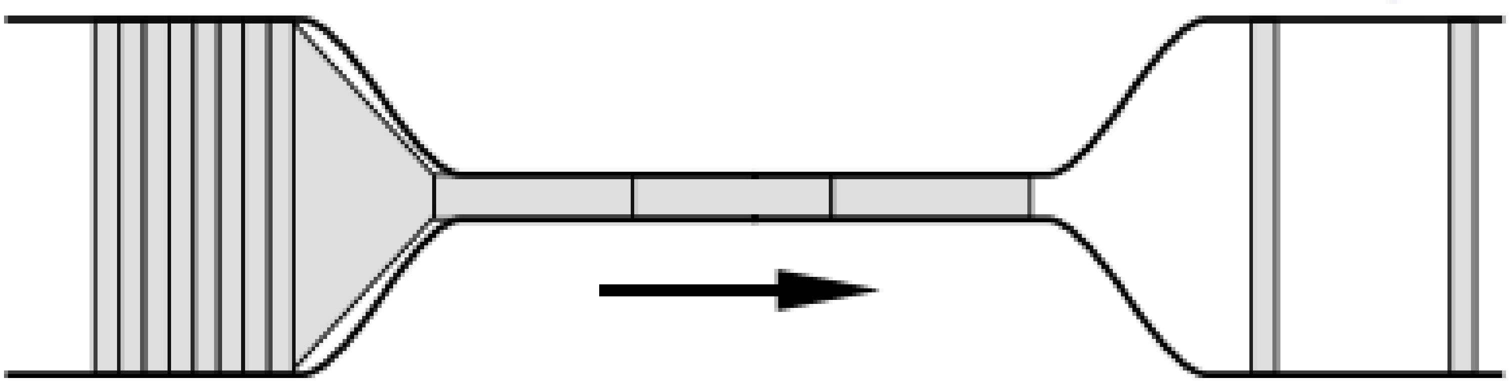
So: Admission Control?

- IP packets, e-mail messages, blog comments –
  - *Anybody can send anything*
  - *Anybody can forge anything*
- We have given up on stopping it at the far end
  - *So, more passwords, password managers*
- See also BGP
  - Internet routing/reachability protocol
  - Effectively unsecure today

So, Edge Device Quality?

- Marketing & sales beats quality every time
  - *Anybody can connect anything*
- QA budget shrinks at scale; only TTM matters
  - QA for a automobile tech: maybe $100/unit
  - QA for a Smart Phone: maybe $3/unit
  - QA for a CPE (cable/dsl/wireless): maybe $1/unit
  - QA for an embedded IoT device: maybe 5₵/unit
- Note: 5₵/unit would be enough, *iff* up front

Congestion (Thanks: Van Jacobson)

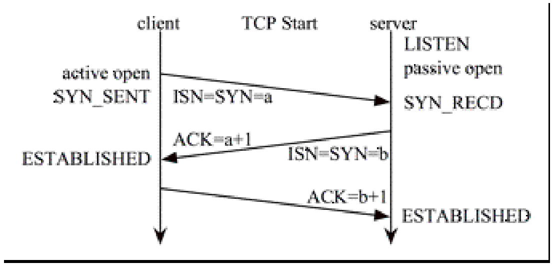


So, Buffering?

- TCP uses congestion to control transmit timing
  - (approx: transmit until loss occurs; slow down)
- Large buffers hide congestion
  - Large buffers are *everywhere*
  - CPE devices, device drivers, backbone routers
- Result: a busy WLAN should deliver ~1/n
  - What we actually get is often closer to ~1/(n^2)
- Installed base is huge; must be *replaced*

TCP Listeners as DDoS Amplifiers

- TCP SYN occupies one octet of sequence space
  - TCP SYN+ACK, likewise
  - This *required* by TCP
  - TCP is *required* by the Internet



- TCP requires retransmission until ACK
  - Including the SYN, *and* the SYN+ACK
- So, every TCP listener is a 3x..20x amplifier
  - Problematic, even when not sent back-to-back

What’s Being Done?

- Reputation technology (RBL, DNSBL, RPZ, etc)
  - Domain names are roughly *too cheap to meter*
  - So, we now have DNS and IP poisoning *at scale*
- Adding state to the edge of the network
  - Rate limiting (e.g., DNS RRL)
  - What about TCP SYN-ACK? (And ICMP and NTP?)
- Shall we allow explicit + disallow unknown?
  - Lengthens deployment curve on new technology

Recommendations

- Disrupt nation-state backed attackers
  - Some countries have earned Internet isolation
- Increase compliance burden for device mfrs
  - Set a floor on quality and thus the QA budget
- Increase compliance burden for ISP’s, telcos
  - Source Address Validation may have to be law
- Consider Dan Geer’s recent proposal
  - A non-patchable embedded device would *expire*

Thank you!

Questions?