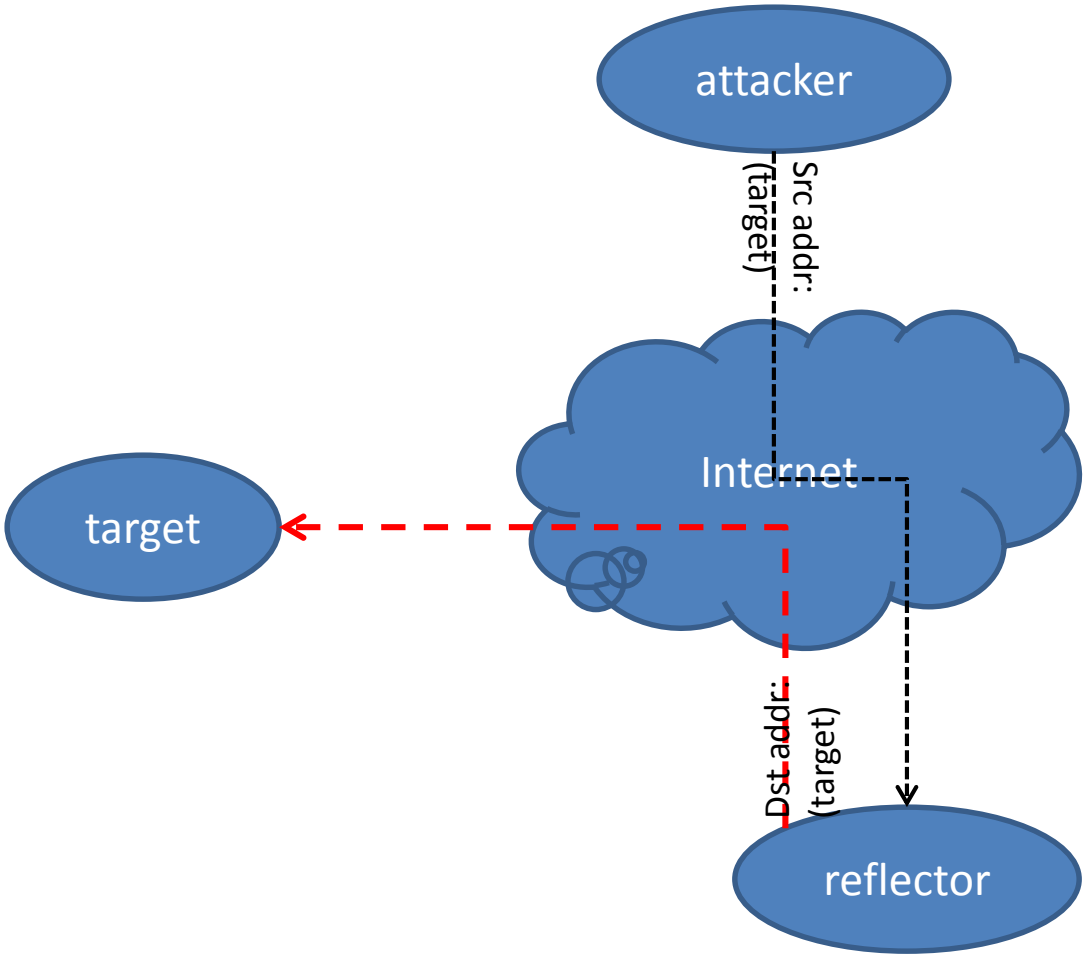
Source Address Validation *Everywhere*

Paul Vixie, CEO
Farsight Security
2014-09-15

The Year 2002's 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
    - (After RFC2267, P. Ferguson, D. Senie, January 1998)

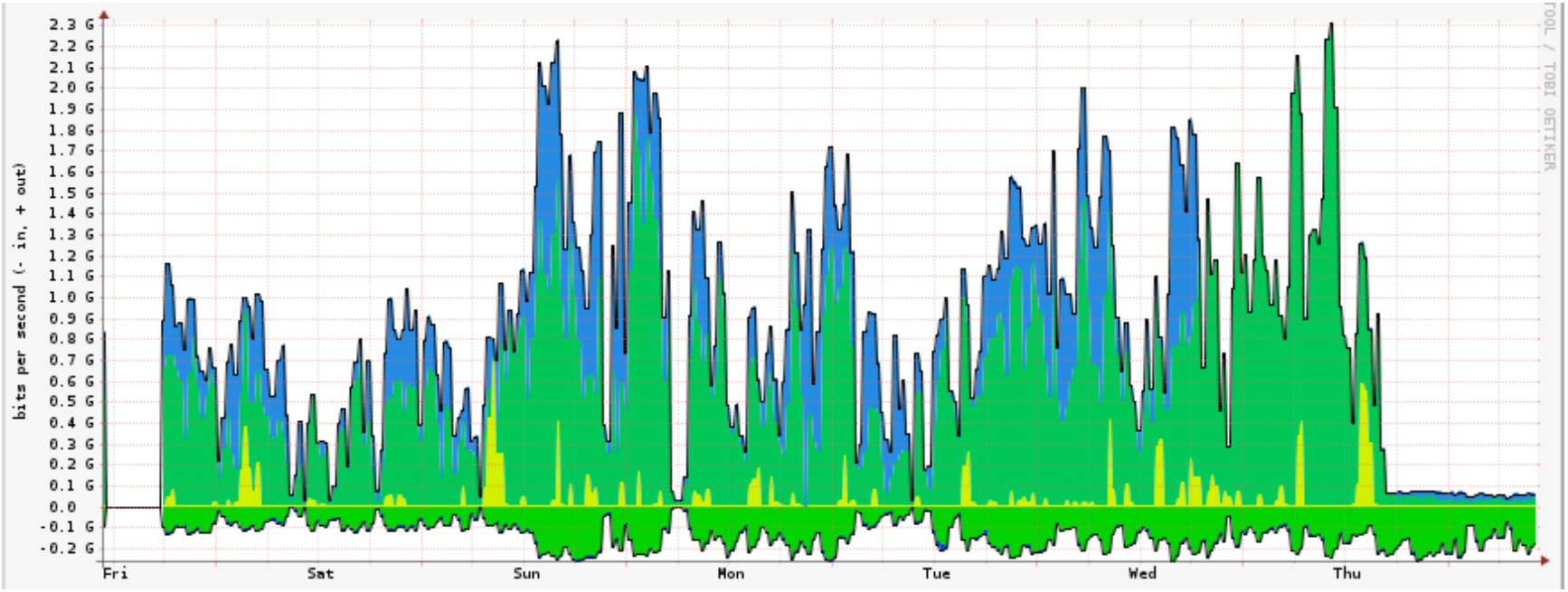
Spoofed Source Attacks



Hopeless Trends

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

Hopeful Sign: DNS RRL



Ode to David Isenberg

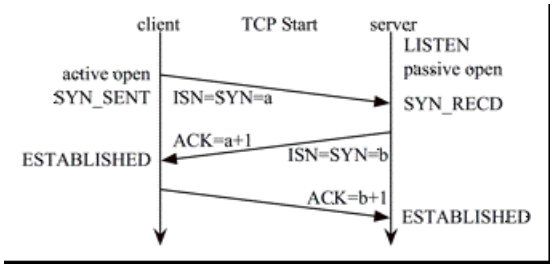
- *Rise of the Stupid Network,* 1997:
  - "Why the Intelligent Network was once a good idea, but isn't anymore. One telephone company nerd's odd perspective on the changing value proposition"
- David was right. We needed to innovate at the edge, and the core had to be assumption-free.
- So, the core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

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

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

Technical Remediation

- Near-end bandaids
  - Stateful rate limiting (e.g., DNS RRL)
  - Maybe TCP should only re-xmit when synch'ed?
  - Something's got to be done about ICMP
  - …and about NTP and all other UDP protocols
- Far-end solutions are far cheaper overall
  - Source Address Validation Everywhere (*SAVE*)
  - Make it the default; exceptions for multihoming

Nontechnical Remediation

- 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?