Improving Internet Security Through Cooperation: SIE Europe in 2018

Dr. Paul Vixie, CEO
Farsight Security, Inc.

Trex, Tampere FI, 2018-06-15

Abstract

- The digital ecosystem known as The Internet uniquely requires cooperation as a precondition for success or relevance, even among competitors. While creativity in interpretation of norms and boundaries can lead to short term successes, such creativity is made possibly only by those norms and boundaries. The Internet ultimately requires that competitors cooperate in order to succeed. One controversial form of cooperation is the sharing of security related telemetry in real time, for the good of all, and also for the good of whoever shares. Dr. Paul Vixie will explain how the Security Information Exchange (S.I.E.) project facilitates such cooperation.

Competition: Universal and Inevitable

- For efficiency and progress, it is necessary for actors to compete:
  - Nations: *influence*
  - Companies: *profit*
  - People: *lifestyle*
- To be constructive, competition must be within a defined framework:
  - Rule of law, irrespective of wealth or other power
  - Recognition of rights: individual, sovereign, and property
  - Standards, such as currency or Internet protocols
- So, there is a balance between competition and cooperation:
  - What's good for all may sometimes also be good for each

Non-cooperation and the Internet

- Cooperation can sometimes be mandated: laws, treaties, norms
  - Enforcement underlies future trust
- In the Internet, nothing can be universally mandated
  - Censorship is treated as damage
- Internet non-cooperation examples: spam, facilitation, e-crime
  - Many new forms of activity are made possible by the Internet
- Importantly, the Internet, and Internet crime, is timely but placeless
  - An activity can be instantaneous, international, and non-consensual

Sharing of Internet Threat Tracking Data

- An attack on one will become an attack on all
  - Our activities cannot be safer than our partners'
- Disclosure of vulnerabilities, attacks, and attackers makes us stronger
  - Even at some cost in prestige
- Sharing of baseline telemetry (*every day* activities) is also necessary
  - Anomaly detection relies on a corpus of common patterns
  - Investigation and recourse rely on knowledge of the whole system
- Personally Identifiable Information (PII) must be avoided
  - Rights of individuals, companies, and nations require privacy *norms*

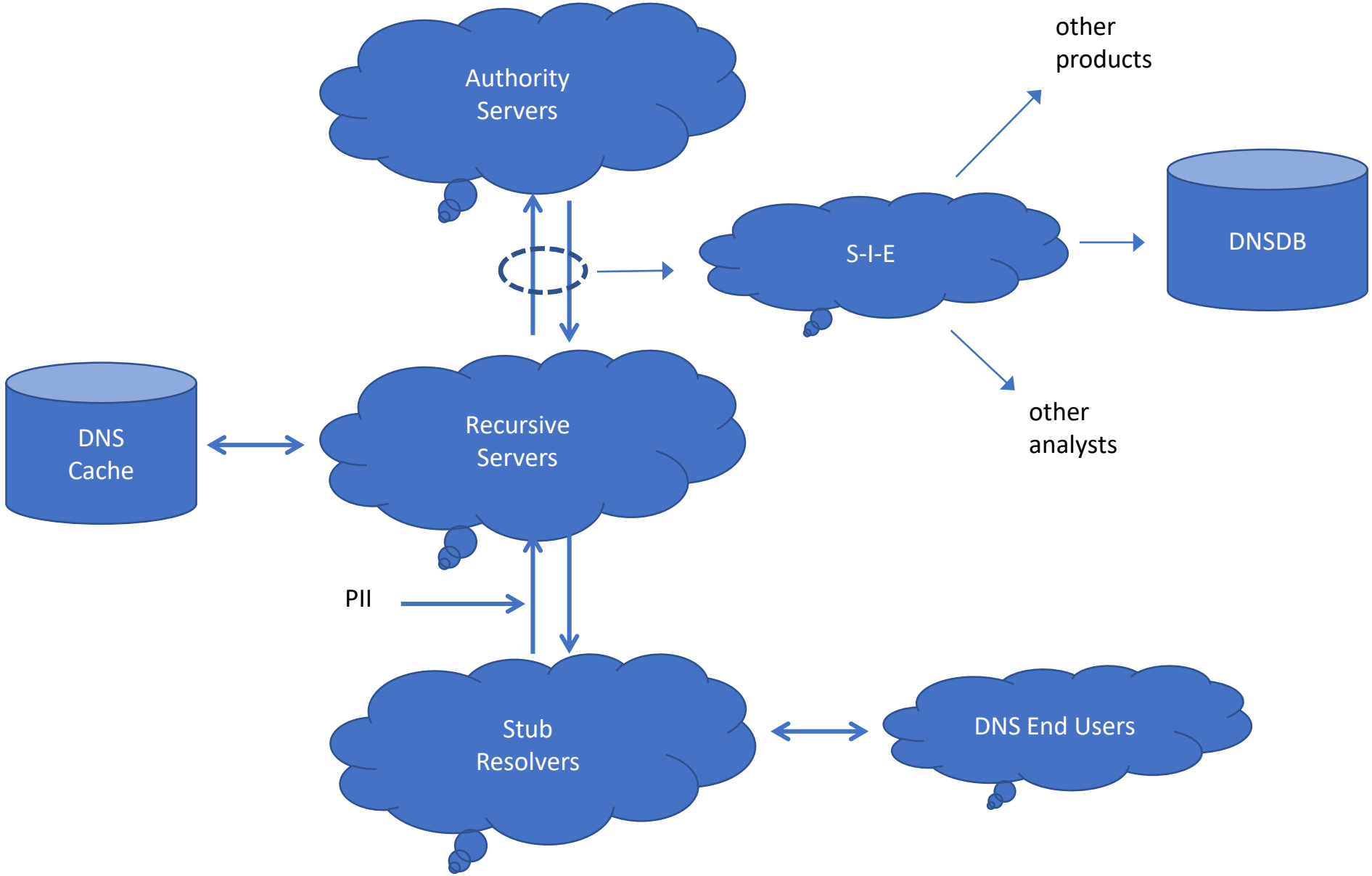
Deliberate Non-Illegal Attacks: *Out of Scope*

- Individuals, companies, and nations sometimes attack others
  - “No-one is a villain in their own eyes.” – Robert Heinlein
- Individuals might *hack back* as a form of self-defense
- Companies might deliberately blur the definition of PII
- Nations might digitally infiltrate other nations (for *parity*?)

- These matters are out of scope for this presentation
  - Noting, even in such cases, general threat and data sharing is still a *net good*

Security Information Exchange (S-I-E)

- In 2007, ISC.ORG launched S-I-E, a not-for-profit global network
  - Sensors everywhere, on a hub/spoke model
  - Hubs offered Internet collocation for analysts
- In 2013, this activity was moved to FARSIGHTSECURITY.COM (new)
  - All security-related sensors, software, data, and contracts were included
- Now in 2018, the S-I-E network size and capacity is ~8X larger
  - Analysts still include academic, commercial, and government
  - Unpaid analysts who charge no fee for their results still have free access
  - End-user information (PII) is still not welcome in the S-I-E cloud


Authority
Servers
other
products
S-I-E
DNSDB
DNS
Cache
Recursive
Servers
other
analysts
PII
Stub
Resolvers
DNS End Users

2018: SIE Europe

- Non-profit limited liability company, incorporated in Germany
  - Founders/owners: Paul Vixie (FSI), Christoph Fischer (BFK), Peter Kruse (CSIS)
  - BFK (hosting) and FSI (devops) will operate the infrastructure (cost recovery)
- Collect data from European participants (academic and commercial)
  - Raw and filtered real time data will remain inside GDPR-governed territory
- Give a little; get a lot: participants will get access to combined data
  - Raw, filtered, or deduped (LAN/UDP or AXA/TCP); or stored (DNSDB API)
- Constraints on redistribution and derivative works
  - No redistribution of raw, filtered, deduped, or stored forms except by FSI
  - Derivative works must remain in Europe or be artificially delayed
- Launched March 2018; testing in April; production by May

TTFN