The Responsible Internet

Cristian Hesselman

Top Team ICT Strategy Day
Utrecht, the Netherlands
June 24, 2022
Agenda

• The Internet infrastructure

• Two problems: black box nature and centralization

• The Responsible Internet and example building blocks

• Strategy suggestions

• Discussion
The Internet infrastructure
High-level operation of the Internet infrastructure

Per-AS planning and coordination, no central authority
Strategic developments

• Ever increasing dependency on the Internet infrastructure for citizens, organizations, society

• Vision: will eventually also serve cyber-physical systems such as smart grids, tele-robots, ITSs

• The Internet and societal systems increasingly co-develop (e.g., strategic digital autonomy, IoT security, DNS4EU)

• Many challenges going forward, such as security, manageability, sustainability

O’Hara, K., Hall, W.: Four Internets: Considering the merits of several models and approaches to Internet governance”. Communications of the ACM 63, 3 (2020)
Two problems of the Internet infrastructure
Problem #1: it’s a black box for users

- Traditional focus on uninterrupted and seamless connectivity
- No insight in nor notification of route changes
- Such as in terms of operators, vendors, security, jurisdictions
- No control over response (e.g., stop transmission or reroute)

- Downside: data might travel through untrusted networks
- Store data, metadata analysis, disrupting equipment or data
- Potentially huge impact on society
- Particularly relevant for cyberphysical/OT services (safety)

- Reduced **trust** in the foundations of our digital society
Problem #2: increasing centralization

- Internet designed to be “in the hands of many”
  - Decentralized and distributed ownership and control
  - Resilience through diversity

- Under pressure due to market concentration
  - A few large powerful players, often non-EU
  - Operators (e.g., DNS, CAs, time) and vendors
  - Pro: quickly introduce new technologies at scale

- Risk for the resilience of the Internet and that of society (knowledge, data, technologies elsewhere)
What does it take to address these problems and enable a more trusted and resilient Internet infrastructure?
Approach: the Responsible Internet

• New security-enhancing properties: transparency, accountability, controllability

• Open software, hardware, protocols, designs (≈TRL7)

• Open Internet measurements (exogenous)

• Added value for critical infrastructure operators, network operators, policy makers, individuals
Inspiration: responsible AI and GAIA-X

Data

You, me, and everyone else
Citizens, organizations, society at large
Hypothesis: empowered users

IBM, Google, Microsoft, universities
Services, algorithms (data in use)
Responsible AI

Amazon, Microsoft, Google, IBM, Oracle
Storage (data at rest)
GAIA-X

Google, Akamai, Telia, KPN, SIDN
Network (data in transit)
Responsible Internet
### Examples of required mechanisms

<table>
<thead>
<tr>
<th>Building block</th>
<th>Examples of mechanisms</th>
</tr>
</thead>
</table>
| Controllability | - Descriptions of path security requirements  
                   - Path-aware technologies (e.g., SCION or segment routing)  
                   - Virtual Network Functions (VNFs) |
| Accountability  | - Append-only distributed logging (cf. certificate logs)  
                   - Scalable path validation  
                   - Cross-measurements from multiple vantage points |
| Transparency     | - Network scopes, network-level data exchanges  
                   - Active measurements (e.g., OpenINTEL), in-band telemetry  
                   - Self-descriptions (cf. GAIA-X and “cybersecurity labels”) |
| Incentives       | - Pilots and lessons learned with “vertical” use cases  
                   - New CAT-based applications and business models  
                   - Insight in investments and operational costs |
| Policy           | - Standardized CAT levels  
                   - Policy models (voluntarily, regulated, (inter)national)  
                   - Policy bodies (cf. MANRS or ICANN) |
Example building blocks
Inter-domain path validation

- Users get a cryptographically signed “receipt” of how their data flows through the network.

- When it changes, they can stop transmission or redirect data through a different path.

- Hypothesis: benefits applications with higher security requirements.

- Challenges: technical design, security vs. transparency, scoped deployment.

CATRIN and UPIN received funding from the Dutch Research Council (NWO).
Inter-domain path control

UPIN received funding from the Dutch Research Council (NWO)
SCION-based networks

Client constructs end-to-end path using segments 1, 2, 3 (interacts with path servers)

Beaconing to discover paths, S selects its valid AS paths to core

AS path (S-P-M-...) in data packet headers + 8 bit message auth code

Name: www.example.net
Address: <ISD, AS, loc_addr>
Data exchange between network operators (DDoS)

This work was funded by the European Union’s Horizon 2020 Research and Innovation program under Grant Agreement No 830927
P4 testbed

• Equipment uses open software and open programmable hardware (e.g., P4-based)

• Enables transparency and experimentation with new data plane functions (e.g., PCFS)

• Explore and learn from “clean slate” architectures such as SCION (e.g., SCION-in-P4)
Open Internet measurements

- Measurement infrastructures:
  - OpenINTEL
  - ENTRADA
  - RIPE ATLAS
  - DMAP
  - LG servers

Stats.sidnlabs.nl

De staat van .nl, 2021

Source: https://blog.apnic.net/2022/02/11/opinion-dns4eu/
Strategy suggestions

• A trusted and resilient Internet infrastructure requires additional properties from the network – opportunity to set up a European networking industry in niche areas

• Set up “moon shot” Internet infrastructure testbeds to start and grow the ecosystem
  • Such as the Responsible Internet or the Extensible Internet
  • One joint national research program (e.g., NGF-based)
  • Potential starting points: CATRIN project, 2STiC, TUCCR

• Unlock Internet security and evolution measurements by setting up a portal for policy makers, tech journalists, and others
Discussion

www.sidnlabs.nl | stats.sidnlabs.nl