Increasing Internet security by bridging research and operations

Cristian Hesselman

NLUUG spring conference
Utrecht, May 11, 2023
Internet security focused on availability (as in CIA)

1. Internet communication must continue despite loss of networks or gateways.
2. The Internet must support multiple types of communications services.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit distributed management of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. The resources used in the Internet architecture must be accountable.

https://www.cidr-report.org/as2.0/
Today’s goal

• Showcase how we increase security of the Internet infrastructure by bridging the worlds of research and operations

• Get your feedback on a few of our long-term Internet research concepts (as apposed to short-term reality)
The Internet
(I assume we can skip this part, but just in case)
The invisible foundation of our digital world

Citizens, organizations, society at large

Services, algorithms (data in use)

Storage (data at rest)

Internet (data in transit)

"Internet" in everyday language

"Internet infrastructure" to avoid confusion

Under the hood: names, numbers, routes, time

References: [1-4]

The Internet hourglass

Most people

Orgs such as SIDN, RIPE, ICANN, IETF

Services

Names, addresses, routes, transports

Transmission

LTE 3G WiFi Ethernet DOCSIS DSL Radio Coaxial Fiber Twisted Pair

TCP UDP HTTP SMTP NTP DHCP DNS SIP
SIDN and SIDN Labs
SIDN is the operator of the .nl top-level domain

• Not-for-profit private organization for the benefit of Dutch society (public role)

• Securely manage .nl, the Dutch national extension on the internet (63% market share)

• Critical service provider: DNS infrastructure and domain name registration (6.3M names)

• Increase the value of the Internet in the Netherlands and elsewhere
SIDN Labs is the research arm of SIDN

- Goal: increase Internet infrastructure security through applied technical research, special focus on .nl and the Netherlands

- Themes: domain name security, infrastructure security, emerging Internet technologies (long term research)

- Types of work: large-scale measurement studies, system design, prototyping and evaluation, contribution to standards

- Results publicly available to advance the Internet

- Bridge between academic and operational world/industry
Internet security: 8 case studies
Details: www.sidnlabs.nl
Case study #1: online impersonation

- We developed Logomotive, a tool that crawls the .nl zone and detects logo usage

- Pilots with Dutch Government (DPC) and Thuiswinkel Waarborg

- Results:
  - Several sites removed from the zone
  - Dashboard in use at SIDN’s anti-abuse desk
  - Logomotive part of SIDN’s BrandGuard service
  - Peer-reviewed paper at PAM2022, blogs
Case study #2: fake web shops

- Sales of fake shoes was a big problem in the .nl zone back in 2016-2018

- Developed tools to detect fake shops, partnered with registrars and ISC to remove them

- Results:
  - Fake shops virtually gone from the .nl zone
  - Increased online safety for users
  - Dashboard in use at SIDN’s anti-abuse desk
  - Peer-reviewed paper at PAM2020, blogs

<table>
<thead>
<tr>
<th>Year</th>
<th>Taken down</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022</td>
<td>199</td>
</tr>
<tr>
<td>2021</td>
<td>224</td>
</tr>
<tr>
<td>2020</td>
<td>481</td>
</tr>
<tr>
<td>2019</td>
<td>4,340</td>
</tr>
<tr>
<td>2018</td>
<td>~12,000</td>
</tr>
</tbody>
</table>
Case study #3: registration checker (RegCheck)

- Abuse regularly involves recent registrations

- We developed RegCheck for and with SIDN’s abuse analysts to quickly inspect such domains

- Results:
  - Daily used “production prototype”
  - 3 machine learning models based on abuse reports (phishing, fake webshops, etc.)
  - User interface that gives hints about algorithm’s decisions (explainable ML)

- Follow-up project with DNS Belgium (.be TLD)
Case study #4: anycast testbed

• Send traffic to any of a set of the same nodes at different locations => increase availability

• SIDN Labs’ anycast testbed
  • 30 sites across the globe
  • Dynamically add/remove nodes
  • Catchment heatmaps
  • any.time.nl and other experimental services
  • http://dnstest.nl/anycast2020/

• Blueprint for .nl’s production anycast infrastructure, measurements with academia
Case study #5: large-scale DNS measurements

• Help operators to make empirically-grounded DNS engineering choices (RFC9199)

• We carried out 6 studies with University of Twente and University of Southern California

• Results:
  • Reengineering of SIDN’s DNS infra
  • Recommendations for Dutch government’s DNS
  • Anteater tool for DNS operators
  • 6 peer-reviewed papers, RFC9199, blogs
Case study #6: TimeNL

- Accurate time is crucial for many security applications (e.g., DNSSEC, OTTP, RPKI)

- Public NTP services often ill-documented (e.g., used time sources, support levels)

- We set up TimeNL, our transparent and well-managed public NTP service

- Results: time.nl, nts.time.nl, ntp.time.nl (in Arnhem, NL), any.time.nl (anycast)

- More NTP traffic than DNS traffic for .nl 😊
Case study #7: DDoS Clearing House

• Increase level DDoS proactiveness for (critical) service providers

• Joint work with: SURF, UT, Telecom Italia, Uni Zürich, Siemens, FORTH, NL-ADC

• Results:
  • Technical pilots in the Netherlands and Italy
  • Transition to production at NBIP (in progress)
  • Testbed, also to be used as a “cyber range”
  • Cookbook and scientific paper (in progress)

This work was funded by the European Union’s Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/
Case study #8: SCION experiments

• SCION aims to improve security of inter-domain routing and isolation of compromise

• Our goal: assess to what extent SCION concepts can improve Internet security

• Results
  • Connection to SCIONlab at ETH Zurich, P4 implementation of the SCION data plane
  • Taught students about SCION at University of Twente and University of Amsterdam

• Work in progress: SCION-NL testbed, interconnecting SURF, UvA, SIDN Labs
Long-term Internet research
Vision: future Internet applications

https://www.youtube.com/watch?v=-7xg3DQyOXw
Hypothesis: require a revised networking paradigm

Increased digital autonomy
More data autonomy for users/service providers
Data-driven policy making
Joint incident analysis for network operators
Push back on Internet centralization

New levels of trust:
“Internet bill of materials”: CAT
In addition to classical Internet security: CIA

Open designs:
Open source
Open hardware
Open data
Best operational practices
Legal & governance

Trusted Open Networking
A more transparent and controllable Internet

- Transparency: logical, cryptographically verifiable data paths and “map” of the macro-level structure of the Internet
- Controllability: route data paths “around” untrusted networks or modify networks to increase resilience
- In addition to existing Internet properties, such as open, generic, distributed and decentralized
- Hypothesis: benefits critical infra, network operators, public policy makers, individuals

References: [6] (concept) and [7] [8] [9] [10] (potential benefits)
Network operator coalitions

• Proposed mechanism to validate value of CAT properties
  • If it works, then consider building it into the Internet’s design (commitment first), unlike “clean slates”
  • Inspired by existing operator coalitions such as MANRS, NL-ADC, and SCION ISDs

• Collaborative inter-domain (security) services, such as
  • Fine-grained sharing of network properties (e.g., measurements, equipment types, jurisdiction)
  • Single-operator-like functions such as path validation, path control, packet processing (e.g., caching)

• Also helps counterbalancing hyperscalers’ global WANs, such as those run by Google, Microsoft, Akamai
AS Information Service (ASIS)

- Self-hosted system for an AS to share interoperability and policy information, such as within a network operator coalition

- Disadvantages of current systems such as WHOIS/RDAP and PeeringDB:
  - Public only; lack of access control
  - Centralized
  - Rate-limited

- Result: prototype in our lab network, let us know if you’d like to work with us

<table>
<thead>
<tr>
<th>Examples of ASIS information types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical contact information</td>
</tr>
<tr>
<td>Security contact information (“AS-wide security.txt”)</td>
</tr>
<tr>
<td>Routing policies and BGP communities</td>
</tr>
<tr>
<td>Preferred peering locations and methods</td>
</tr>
<tr>
<td>Which data laws apply to the network</td>
</tr>
<tr>
<td>Information useful for path control and planning</td>
</tr>
<tr>
<td>Information about energy footprint of devices</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

UNIVERSITY OF TWENTE
CATRIN project: a small-scale responsible Internet

- www.catrin.nl: 1.9M Euros from NWO, 7 Ph.D. students, 11 partners from NL, 8 international

- Design and prototyping of network descriptions, protocol extensions, evaluation via test networks

- Developing value-added service designs for network operators and enabling them to enhance the public Internet

- Validation with organizations and individuals (e.g., via browser extensions)

This research received funding from the Dutch Research Council (NWO) as part of the CATRIN project
Further strengthening NL as an Internet hub

• Vision of the Internet of 2040 and its security developed by a strong, organized tech community that combines research, policy and operations

• Open federated measurement infrastructure for the ongoing analysis of Internet infrastructure robustness (cables, routing, DNS, time) with a multidisciplinary user community

• Open federated experimental network to develop, evaluate and translate new security concepts into solutions based on a “commitment first” principle
Goal: reinforced Dutch Internet community

Society
- Citizens
- Companies
- Governments

Internet infrastructure
- Operators
- Standards
- Regulators
- Manufacturers
- Research
- Education

Services, algorithms/AI, data (examples)
- Messaging
- Search
- E-commerce
- Mobility
- Energy
- Tele-robotics

Vision
- Data platform
- Test network

ICANN
RIPE
OARC
CENTR
GÉANT

DADI
EU

ACCSS
TUCCR
2STiC

IETF
IRTF
FvS

UvA
UT
TUD
CVD

UNIVERSITY
OF
TWENTE.
Lessons learned in crossing the bridge
A few lessons learned about technology transfer

• Define problems and validate preliminary results with (external) users/domain experts

• Set up long-term relationships with academia and research labs (e.g., by seconding staff)

• Combine scientists, engineers, and operators (in one team/under one roof if possible)

• Set up a dedicated (joint) research network, such as for measurements, prototypes, pilots

• Make results generic and public, apply them yourself (“eat your own dogfood”)

• Keep in mind that peer-reviewed publications are a means, not a goal
References