IP Address and Cross-border Cooperation for Resolving the Cyber Attribution Challenge

Eun Chang Choi
eunchang.choi@aya.yale.edu
Table of Contents

Cyber Attack Maps: Global Scale
What Makes an IP Address untraceable?
IP Addresses Spoofing, VNC (Virtual Network Computing)
Why Cyber Attacks Are So Difficult to Trace
The Difference of IP Address, Real Location, Borderline, and National Jurisdictions
Why are IP Addresses at Odds with Jurisdiction?
Attack Traffic Overview

Displayed are the current number of network attacks by major geographic region (State or Country). Highest volume regions are called out below.
Count of DNS(SHODAN) Nodes vs. IP address assigned to ccTLD

ODR: \( y = (1.08 \pm 0.03)x + (-3.44 \pm 0.18) \), Residual Variance = 0.12
APCERT cooperates with CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) to ensure internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation.

What’s NEW

31 July 2019
APCERT Drill 2019 – Catastrophic Silent Draining in Enterprise Network updated

28 May 2019
FAQ — Membership/Partnership Updated

9 May 2019
APCERT Annual Report 2018 Released

4 March 2019
FINCSIRT joins APCERT Liaison Partner
FINCSIRT (Financial Sector CSIRT, Sri Lanka)'s Liaison Partnership application has been accepted.
Panasonic PSIRT joins APCERT Corporate Partner
Panasonic PSIRT's Corporate Partnership application has been approved.

24 February 2019
APCERT Policy on Information Sharing and Handling approved

23 October 2018
Results of the APCERT Steering Committee (SC) Election 2018 - Chair: ACSC (2019-2019)
Cooperation of CERTS in Asia-Pacific Regions regardless of borderlines
Exclusive economic
zone claims
That countries believe they are entitled to
under UN Convention on the Law of the Sea

- Philippines
- Vietnam
- Malaysia
- Brunei
- Indonesia

Reclamation work by:
China  Taiwan  Philippines  Vietnam  Malaysia

Sources: amti.csis.org; janes.com; lawfareblog.com
- IP address is used to uniquely identify and locate that system for the purpose of data transmission
- What if IP Numbers are fake?
IP Address Spoofing

Attacker
real IP: 1.1.1.1

Internet-Router
source: 3.3.3.3
destination: 2.2.2.2

source (spoofed): 3.3.3.3
destination: 2.2.2.2

trusted Host
IP: 3.3.3.3
(might be target of DoS-attack)

Victim
IP: 2.2.2.2
(possible security breach)
### IPv4 Network Packet Headers

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>8.8.8.8</td>
<td></td>
</tr>
<tr>
<td>Destination IP Addr</td>
<td>5.6.7.8</td>
<td></td>
</tr>
</tbody>
</table>

**Diagram:**

- **Version**: 4
- **Header Length**: 1
- **Service Type**: 0
- **Total Length**: 0
- **Identification**: 0
- **Flags**: 0
- **Fragment Offset**: 0
- **TTL**: 0
- **Protocol**: 0
- **Header Checksum**: 0
VNC (Virtual Network Computing)

Before IP spoofing, my location is India

After IP spoofing, my location is China
DNS Spoofing

1. Request to Real Website
2. Inject Fake DNS entry
3. Resolve to Fake Website

https://www.keycdn.com/support/dns-spoofing
Address Resolution Protocol Spoofing

Routing under normal operation
- LAN User
- Hub/switch
- LAN Gateway
- Internet

Routing subject to ARP cache poisoning
- LAN User
- Hub/switch
- LAN Gateway
- Internet
- Malicious User
Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers

Sony, Google, RSA and now Citigroup are just some of the prominent victims of cyber attacks as defenses at large organizations prove porous and attackers elude detection.

...invasive attacks on a much more regular basis, but IP address unknown

https://www.sciencemag.org/news/2015/03/seeking-address-why-cyber-attacks-are-so-difficult-to-trace-back-hackers
Top 5 Source IP Address in 2018

- 163.177.152.14
- 123.249.27.191
- 122.155.84.56
- 146.185.222.60
- 176.119.4.34
## IP Information for 146.185.222.60

### Quick Stats

<table>
<thead>
<tr>
<th>IP Location</th>
<th>Russian Federation Saint Petersburg Petersburg Internet Network Ltd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>AS44050 PIN-AS, RU (registered Nov 09, 2007)</td>
</tr>
<tr>
<td>Whois Server</td>
<td>whois.ripe.net</td>
</tr>
<tr>
<td>IP Address</td>
<td>146.185.222.60</td>
</tr>
</tbody>
</table>

% Abuse contact for '146.185.222.0 - 146.185.222.255' is 'abuse@pinspb.ru'

inetnum: 146.185.222.0 - 146.185.222.255
netname: cust17011
country: RU
admin-c: MC40674-RIPE
tech-c: MC40674-RIPE
status: ASSIGNED PA
mnt-by: MNT-PINSUPPORT
created: 2019-08-21T13:08:04Z
last-modified: 2019-08-21T13:08:04Z
source: RIPE
Warning:

We've already warned you, and this is just a beginning. We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the 24th, 11:00 PM (GMT).
False allegation owing to bogus IP address

The Evidence That North Korea Hacked Sony Is Flimsy

- South Korea blamed North Korea for the attack as well as China—since an IP address in China appeared
- …Officials later retracted the allegations.
The WannaCry ransomware outbreak of 2017
Attempts of hacking Lockheed Martin in 2016
The 2016 Bangladesh Central Bank cyber-heist
The breach at Sony Pictures Entertainment in 2014
North Korean Hacker spreaded WannaCry and Trojan.Alphanc using IP address 84.92.36.96 → for “Command-and-Control”
The hardest problem in finding the source of cyber attacks is attribution. You will be trying to find out who's doing it, but purely technical means are insufficient.

Untraceable of IP Addresses
→ Murky Real Physical Location
→ Impossible to Trace Attackers
→ Elusive Quest of Cyber Attribution
determining the actor responsible for a cyberattack

* The body of evidence collected for technical attribution
* Identifying IP address, and conducting extensive forensic investigations,

Source: Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government, RAND Corporation 2019
What makes Cyber Attribution difficult:

- **Untraceable IP Address**. Fake metadata are the Most Potent Weapon in Cyberwar.
- **Lack of end-to-end accountability** in the current Internet infrastructure.
- **Invisibility**: Cyber attacks spanning jurisdictions, networks, and devices are only partially observable from the point of view of a defender.
- **Lack of Jurisdiction** allowing investigation
DARPA calls for help to improve cyber attack attribution

Reliable cyber attack attribution is currently almost impossible, and the Defense Advanced Research Projects Agency (DARPA) wants to find a solution for that problem.

https://www.helpnetsecurity.com/2016/05/10/darpa-cyber-attack-attribution/
Attribution program by U.S. DARPA

TA1
Ground Truth via All-Sources Monitoring

TA2
From Data To Information

TA3
Find Adversary Mistakes

External Information Sources
- Commercial Threat Feed
- OSINT (e.g., social networks)
- Network IDS
- End Host Logs (e.g., HBSS, TC)
- SIGINT

Fuse & Predict

Validation & Enrichment

Shareable Information
Identifying IP Address (Physical Location)

Cyber attribution (determining the actor responsible for a cyberattack)

Identifying National Jurisdiction (by Court)

No Jurisdiction, No Authority, No Law Enforcement

IP Addresses do not recognize National jurisdiction. Both are often mismatched.
The Principality of Sealand with its own National Jurisdiction
PRINCIPALITY OF SEALAND

Sealand was founded as a sovereign Principality in 1967 in international waters, seven miles off the eastern shores of Britain.
Since 1967, SEALNAD claimed its own sovereign nation with its own flag, currency, passports, jurisdictional and legal status. SEALNAD has fired a weapon towards a English government vessel in order to defend their territory. English court found that it lacked jurisdiction over SEALNAD.
Which jurisdiction an unknown IP Address does fall under if a crime is committed using it?

[EXAMPLE] The Silk Road website used TOR that obfuscated user’s real location online. TOR does not use any common Top Level Domain nor IP address.

What country would have jurisdiction to try and shut down the Silk Road website?

Without IP address connected to any domain name, how can any Gov’t authority trace bad guys?
Tor ("The Onion Router") conceals the location and IP address.

Originally designed to protect the identity of U.S. operatives and dissidents in repressive countries like China.
The anonymous Internet

Daily Tor users per 100,000 internet users

- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.ox.ac.uk

Oxford Internet Institute
University of Oxford
After tracing infringement of its copyrights to a particular IP address, Cobbler Nevada, LLC filed a lawsuit against the John Doe IP address for direct and contributory copyright infringement.

[US Court ] Copyright trolls need more than just an IP address if they want to go after copyright infringement. An IP address is not enough proof to tie a person to a crime.

Cobbler Nevada, LLC v. Gonzalez, (9th Cir. United States) 2018
An IP address is not a specific person and may not even be a particular state.
In 2012, federal judge in New York state denied the request of three porn studios to subpoena the names of users of 79 IP addresses.
Tracing IP address to file a lawsuit against the unknown person’s IP address for illegal action, will not be accepted by the Courts.

...because IP address is not enough proof to tie a person to a crime or illegal action.
Court confirms that IP addresses are personal data in some cases.

Collection and further processing of IP addresses would be subject to EU data protection law.

Court of Justice of the European Union
Patrick Breyer v. Germany
IP Addresses at Odds with Jurisdiction

Why national jurisdiction becomes an impediment in cyber attack attribution and investigation?
Jurisdictional Limitations

Jurisdictional limitations can hinder attribution in cross-border cybercrime investigations.

To determine the actor responsible for a cyberattack, every time a law enforcement agency has to undertake an investigation that crosses borders, it must go through official channels to request help.
“How do we collectively develop legal norms that apply in cyber space, while respecting the integrity of national jurisdictions?”
Challenges in Cyber Attribution

1. Hard to find strong evidences for reaching a correct conclusion about the sources of attacks

2. Investigation needs metadata connected to the attack including IP addresses, email data, hosting platforms, domain names. → Fake metadata are generated

3. Untraceable real IP Addresses (easily hidden by VPN Software, Proxy Server, Tor Browser. Changing IP addresses, and using Public Wi-Fi)
4. Linking indications together. Technical, political, and all-source indicators are all tools used in determining cyber attribution.

5. Cyber attackers strongly deny evidences. Courts often relies on physical evidence.

6. Effective cyber attribution investigations cross-borders are being blocked by national jurisdiction.
‘Global Cyber Attribution Consortium’

- International experts provide independent investigation of major cyber incidents for the purpose of attribution.

- Avoid an appearance of bias and to protect transparency

- Work with victims with their cooperation to investigate cyber incidents

- Standardize methodological approaches

https://www.rand.org/pubs/research_reports/RR2081.html
IS IT TIME TO INSTITUTIONALIZE CYBER-ATTRIBUTION?

Posted on August 21, 2018 by Karl Grindal, Brenden Kuerbis, Farzaneh Badii and Milton Mueller

Authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions. New institutions are needed to develop the credibility and procedural checks and balances that can take attribution beyond one nation pointing its finger at one of its adversaries. This white paper explores the attribution challenge, reviews proposed models for new institutions and sketches an agenda for future research.

Keywords—attrition; cybersecurity; forensics; governance; internet; transnational institution