Measuring Unnecessary Exposure of Network Traffic To Nation States

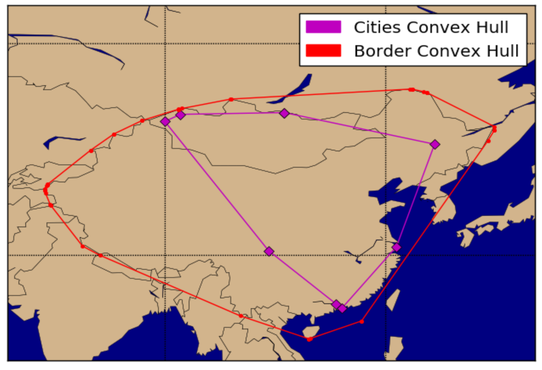
Jordan Holland and Max Schuchard
University of Tennessee, Knoxville

University of Tennessee VOLSEC — COMPUTER SECURITY LAB —

- The logical and geographical topologies of the internet do not necessarily line up
- **Question:** Does the logical topology of make sense geographically?
- **Answer:** In the **majority** of instances it does not.
- Example: a compressed observed traceroute path at a nation level:
  - France → United States → Great Britain → Germany
- Non-logical geographical paths like the example to the left occur frequently, needlessly exposing traffic to extraneous nation states
- **Challenge:** How do we algorithmically measure the irregularity of the geographical topology of the Internet?

- **Challenge:** Need to mathematically define the set of expected countries traffic could be exposed to, which we term *geographically normal*
- **Solution:** Using the *convex hull* between a set of points defining the source country and a set of points defining the destination country

- **Challenge**: A nation's political borders do not necessarily reflect where the bulk of the Internet infrastructure resides
- **Solution:** Define two polygons for each country: one using the political borders of the country, and one using the locations of the 15 most populous cities in each country.



Method

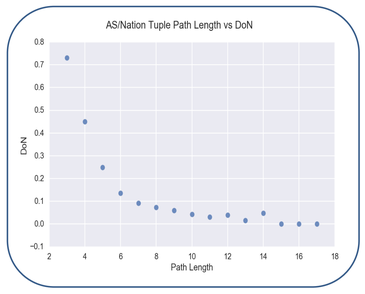
- Examined over 23,000,000 traceroute paths from Ripe Atlas Traceroutes Data
- Mapped each IP address in the path back to an AS/Nation state tuple
- Compressed repeated tuple instances down to a single instance
- Path considered *normal* if no countries outside our previously defined set are found
- Only considered nations and ASes with over 200 traceroutes where they are the source, destination, and transit entity separately.

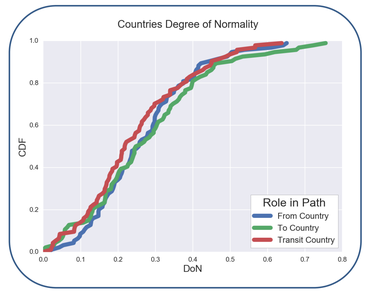
- As a metric of normalcy, we have defined **Degree of Normality (DoN)** as:

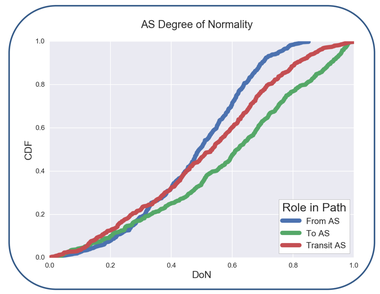
$$DoN = \frac{total\ \text{“}normal\text{”}\ paths\ seen}{total\ paths\ seen}$$

- The DoN over all of the paths examined was 0.409
- **The majority (3 out of 5) paths examined nedlessly expose traffic to extraneous nation states**

General Degree of Normality







Regional Degree of Normality

	Africa	Americas	Asia	Europe	Oceania
DoN From	.1464	.5707	.2356	.4202	.2110
DoN To	.1791	.5807	.1898	.4098	.1404
DoN Transit	.1799	.2849	.1666	.3806	.1507

To \ From	Africa	Americas	Asia	Europe	Oceania
Africa	.2943	.3365	.0663	.1660	.0196
Americas	.1863	.7157	.3829	.5975	.4048
Asia	.0576	.3341	.2091	.1643	.1023
Europe	.1453	.5680	.2043	.4331	.1020
Oceania	.0070	.1928	.1336	.0353	.7620

Examining Degree of Normality Between Each Region

- The Americas have a higher than average DoN when they are the source or destination of a path, but when providing transit for a path they have a *much lower* DoN
- In contrast, Europe sees very little change in DoN given their role in the path

- All regions but Africa and Asia have above average DoN when staying inside the region
- A path from Europe to the Americas has a better chance of being *normal* than a path staying inside Europe
- DoN from one region to another is highly symmetrical

Case Study: Unnecessary Exposure to the Five Eyes

- The Five Eyes is a known intelligence sharing alliance including Australia, Canada, New Zealand, the United Kingdom, and the United States
- The DoN for paths from a Five Eyes country to a Five Eyes country is .471, about 13% higher than the overall average
- Country A *“benefits”* from country B if country B needlessly exposes its traffic to country A, illustrated with the Five Eyes to the left
- 4 out of the 5 members of the Five Eyes are in the top 15 countries that the group *“benefits”* from the most