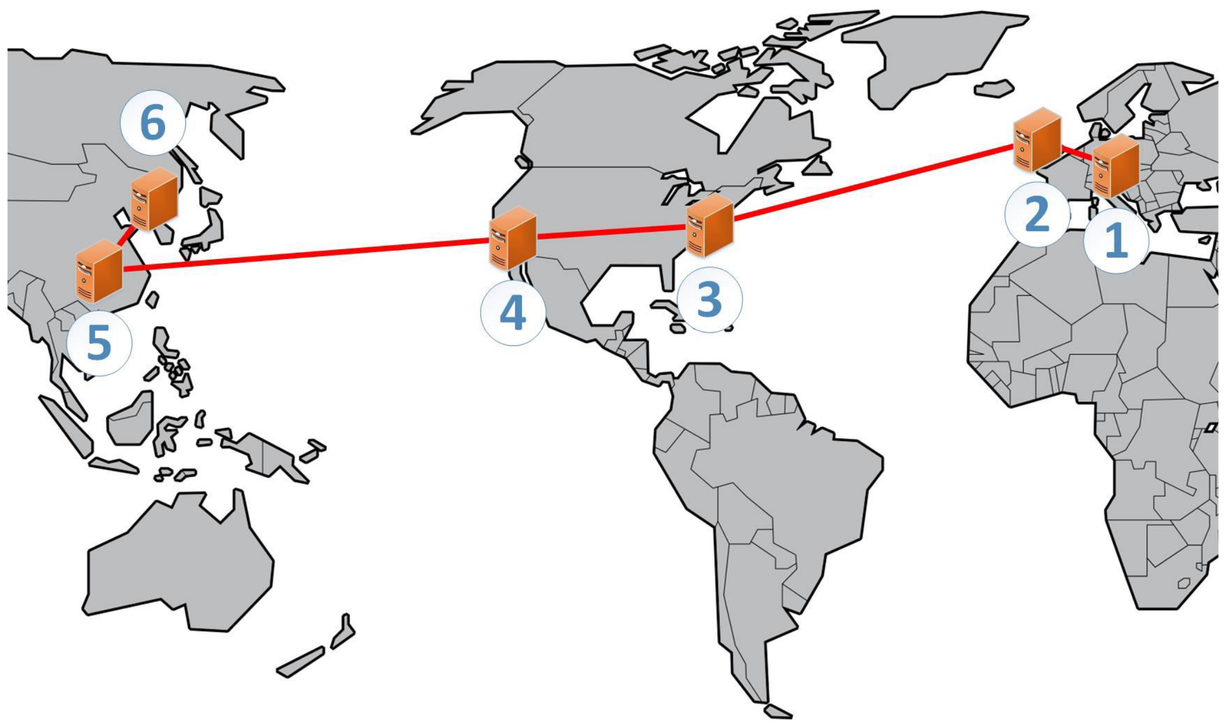
Temasek Defence Systems Institute

Detection of Active Topology Probing Deception

Author: Phua Weiyou Nicholas (ST Electronics)
Thesis Advisor: Dr. Robert Beverly (Naval Postgraduate School)

Objectives of Thesis

- Obtain and analyse past and present traceroute data collected from vantage points across the globe to discover inconsistencies that may reveal the presence of deceptive mechanisms that would invalidate inferred topologies.
- Investigate instances of known ground truth as case studies for classification and verification.



Fake topology presented by The Pirate Bay traceroute in 2013

Main Research Ideas

The following non-exhaustive list acts as potential indicators of an anomaly, which may suggest either intentional or benign manipulation of the interred topology from traceroutes.

- Packet Delay Correlation
- Perceived Geographical Discrepancies
- Continuous Consecutive IP Identification Values
- Autonomous System Link Discrepancies
- Multiple Probe Types
- Multiple Ingress Points
- Common Subnet Hops

The approach is to comb through entries in the 2013 CAIDA IPv4 Routed /24 Topology Dataset [1] to identify traceroutes with certain interesting characteristics, filter and perform additional analysis on them, and compare the findings for equivalent entries in the 2014 dataset.

References:
[1] CAIDA. (2015). The IPv4 Routed /24 Topology Dataset. [Online]. Available: http://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml

Research Results

- Akamai, Korean Telecom and China Telecom Patterns with characteristics suggesting anomalies.
- The Pirate Bay traceroute spoofing is not limited to just one single IP address.
- Naive traceroute deception systems on the Internet may be detected easily.

Benefits of the Research

- Improve cybersecurity defence by building better topology deception systems.
- Improve cyber operations by identifying adversary deception systems.

Future Work

- Identify and analyze specific websites on the Internet instead of combing through all IPv4 addresses.
- Have automatic detection of topology deception systems.

NUS National University of Singapore