Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking

http://www.caida.org/funding/hijacks/

SUMMARY

Recent reports have highlighted incidents of massive **Internet traffic interception executed by re-routing BGP paths across the globe** (affecting banks, governments, entire network service providers, etc.). The potential impact of these attacks can range from massive eavesdropping to identity spoofing or selective content modification.

Because of their complex dynamics, and the number of different actors involved on a global scale, devising effective methodologies for the **detection and characterization of traffic interception events requires empirical and timely data** (e.g., acquired while the event is still ongoing). Such data must be a combination of **passive BGP measurements and active measurements** (such as traceroutes), since the mechanism triggering the attack operates on the inter-domain routing control plane, but the actual impact is only verifiable in the data plane.

In this project we:

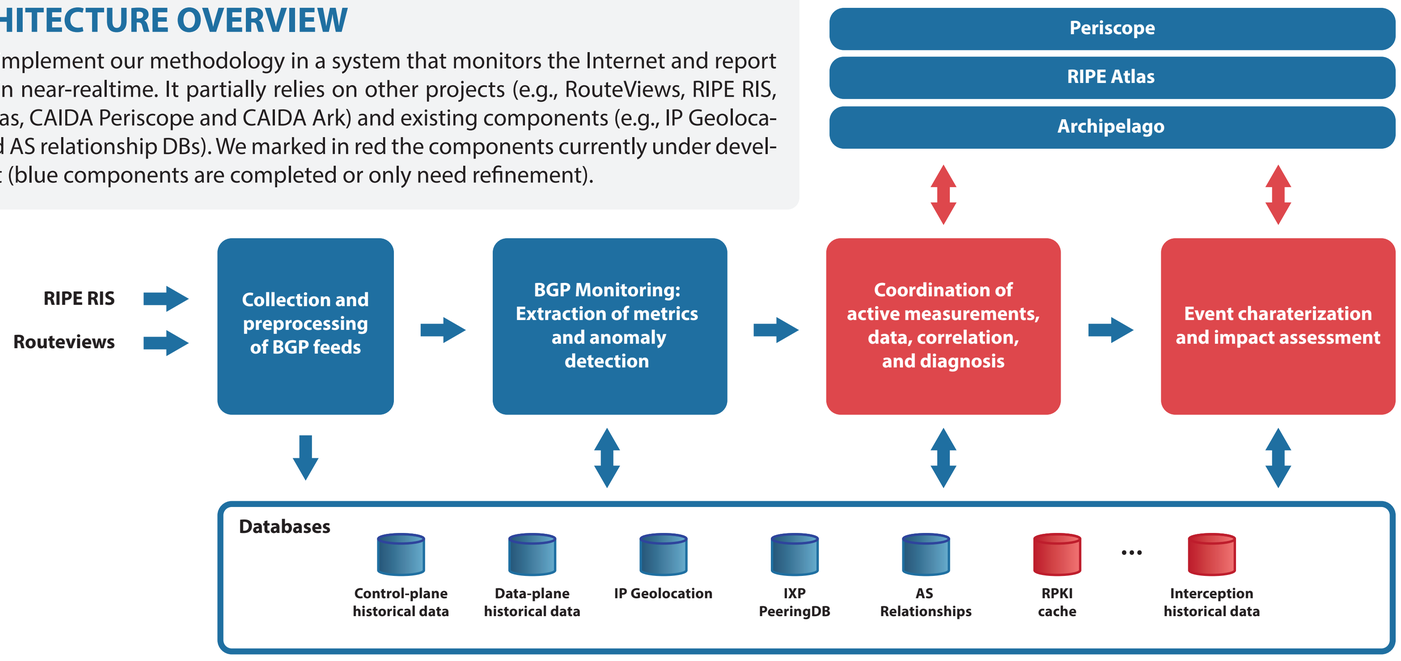
1. investigate, develop, and experimentally evaluate **novel methodologies to automatically detect traffic interception events** and to characterize their extent, frequency, and impact;

2. extend our measurement infrastructure to **detect in near-realtime and report episodes of traffic interception based on BGP hijacking;**

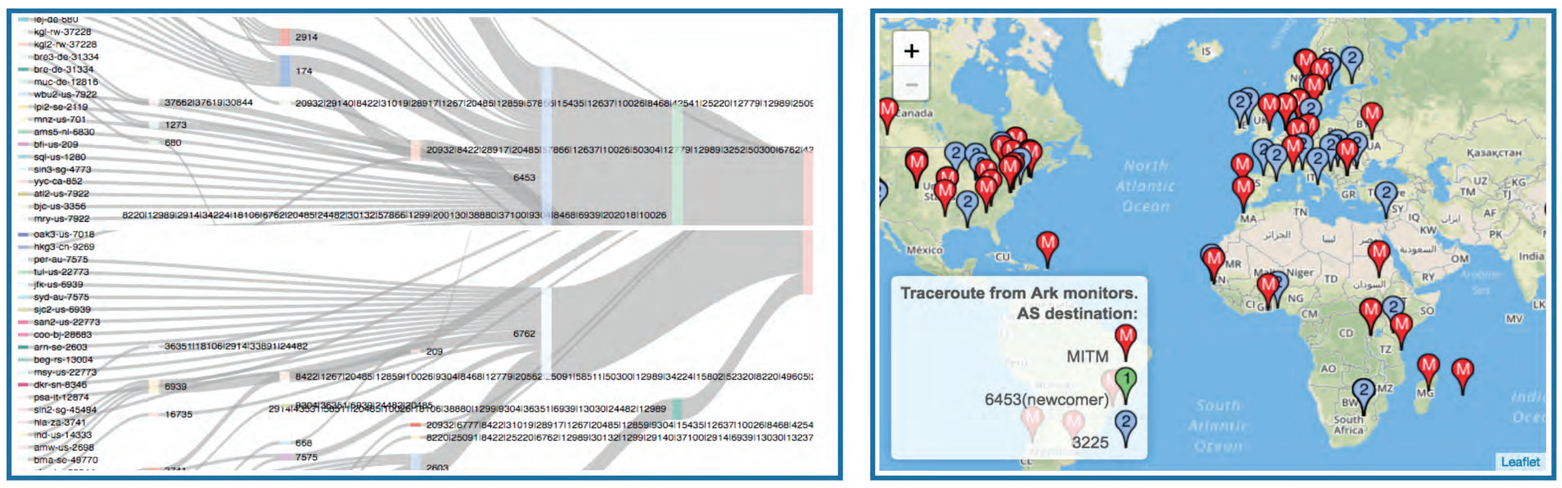
3. document such events, providing datasets to researchers as well as informing operators, emergency-response teams, law-enforcement agencies, and policy makers.

ARCHITECTURE OVERVIEW

We implement our methodology in a system that monitors the Internet and report events in near-realtime. It partially relies on other projects (e.g., RouteViews, RIPE RIS, RIPE Atlas, CAIDA Periscope and CAIDA Ark) and existing components (e.g., IP Geolocation and AS relationship DBs). We marked in red the components currently under development (blue components are completed or only need refinement).

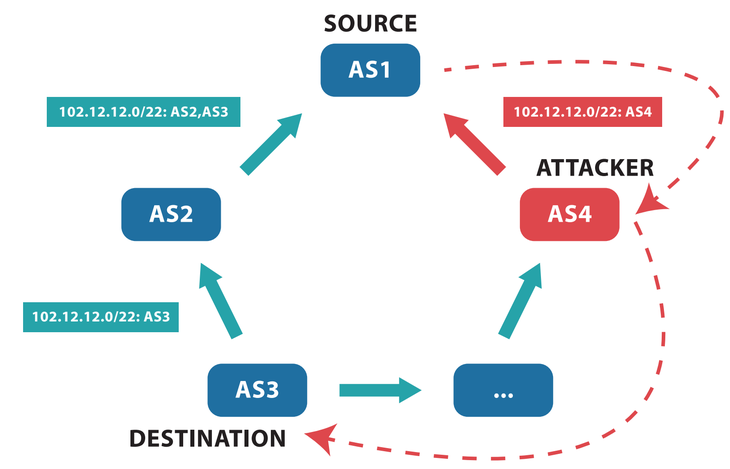


DASHBOARD



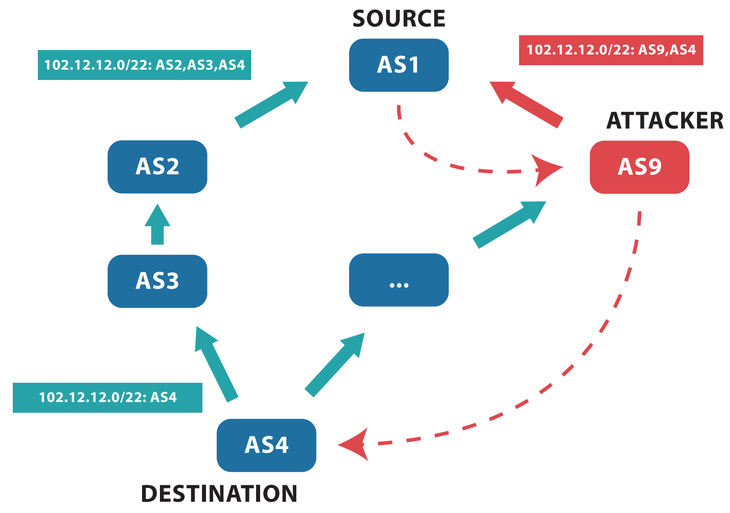
To help understand the events detected by the system, we are developing a dashboard that summarizes geographic and topological information extracted from both control- and data-plane measurements. For example, we display on a map the location of the probes whose traceroutes traverse either the potential victim AS only (blue), or the potential attacker AS only (green), or both (red). We use a Sankey diagram (left) to group path segments observed by multiple monitors, to facilitate detailed characterization.

FAKE ORIGIN
ATTACK SCENARIO 1



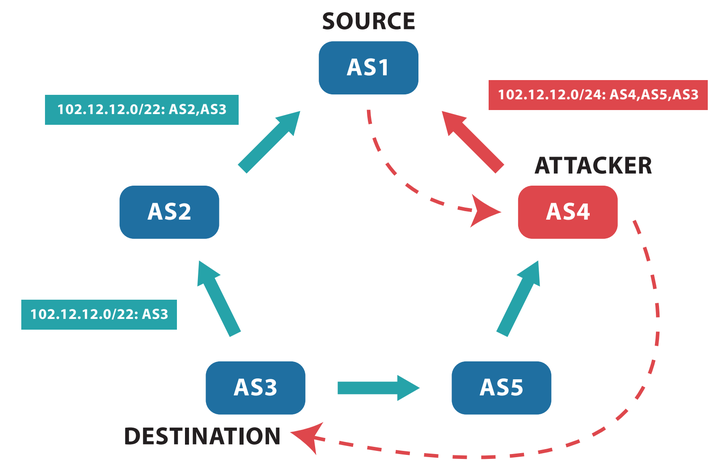
The attacker pretends to be the owner of the prefix but preserves a route through a legitimate path to reach the victim (destination). To detect this attack, we monitor multiple-origin-AS (MOAS) prefixes, filter out cases in which the ASes involved in a MOAS have relationships (e.g., customer-provider) that suggest the event is legitimate, and issue traceroutes from multiple vantage points in order to compare the BGP AS path with the AS path inferred from packet probing. In case of interception these paths will differ.

FAKE PATH
ATTACK SCENARIO 2



In this scenario, the attacker evades MOAS detection by lying about being able to reach the victim (destination) in few hops. To detect this attack, we monitor BGP annoucements looking for edges in the topology graph that were never previously observed. We then execute traceroutes and compare BGP AS paths and AS paths inferred from the data plane as in the previous example.

FAKE SUB-PREFIX ANNOUNCEMENT
ATTACK SCENARIO 3



The attacker announces to its neighbors a sub-prefix of the prefix originated by the victim AS (destination) using the legitimate path (AS4,AS5,AS3). To detect this attack, we check each newly announced sub-prefix and look for the suspicious presence of a common sub-path in all the paths visible through our monitors. In this example, all the paths towards the victim will share the sub-path AS4,AS5,AS3 since neither AS3 or AS5 are announcing such sub-prefix.

TEAM

Alberto Dainotti (Lead PI) | Phillipa Gill (PI) | Alistair King
Ruwaifa Anwar | Danilo Cicalese | Kc Claffy | Dario Rossi | Chiara Orsini

Funding source:

NSF CNS-1423659
DHS S&T HHSP 233201600012C