SPOOFER

BCP 38

SPOOFER.CAIDA.ORG

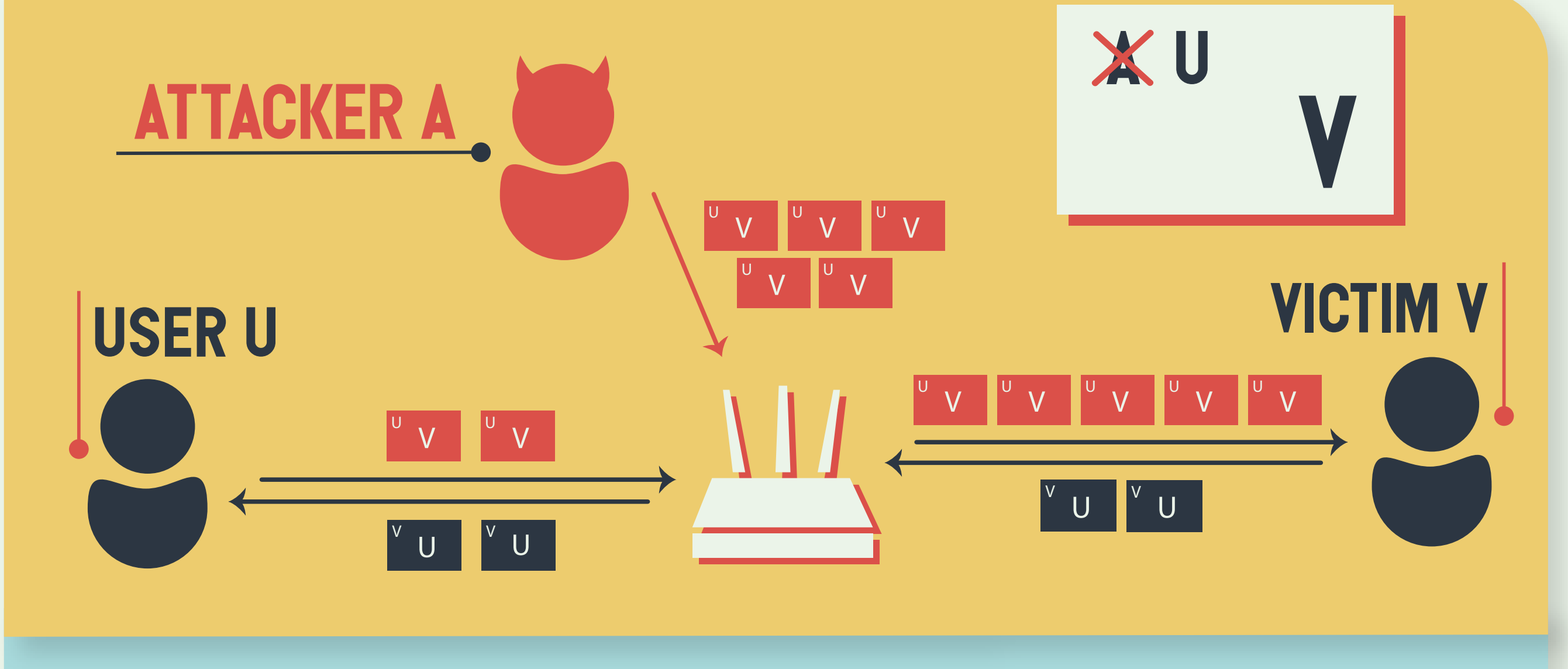
SUMMARY

Seeking to minimize the Internet's susceptibility to spoofed DDoS attacks, DHS has funded CAIDA to develop open-source software tools to assess and report on the deployment of source address validation (SAV) best practices. This project includes applied research, software development, new data analytics, systems integration, operations and maintenance, and an interactive analysis and reporting service. CAIDA's first contribution was to develop and support a new client-server system for Windows, MacOS, and UNIX-like systems that periodically tests a network's ability to both send and receive packets with forged source (spoofed) IP addresses. We are now producing reports and visualizations that will inform operators, response teams, and policy analysts. The test results will allow us to analyze characteristics of networks deploying source address validation (e.g., network location, business type).

WHAT IS SOURCE ADDRESS SPOOFING?

The greatest security vulnerability of the Internet (TCP/IP) architecture is the lack of source address validation, i.e., any sender may put a fake source address in a packet, and the destination-based routing protocols that glue together the global Internet will try to forward that packet to its intended destination. Attackers exploit this vulnerability by sending many (millions of) spoofed-source-address packets to services on the Internet they wish to disrupt (or take offline altogether). Attackers can further leverage intermediate servers to amplify such packets into even larger packets that will cause greater disruption for the same effort on the part of an attacker.

Many years ago, the IETF recommended best practices (BCP38 in 2000 and BCP84 in 2004) to mitigate this vulnerability by configuring routers to validate that source addresses in packets are legitimate. Unfortunately, compliance with such practices is notoriously incentive-incompatible. That is, source address validation (SAV) requires configuration effort, but its deployment helps primarily other networks who are thus protected from spoofed-source attacks from that network. Nonetheless, any network who does not deploy BCP38 is part of the DDoS problem.

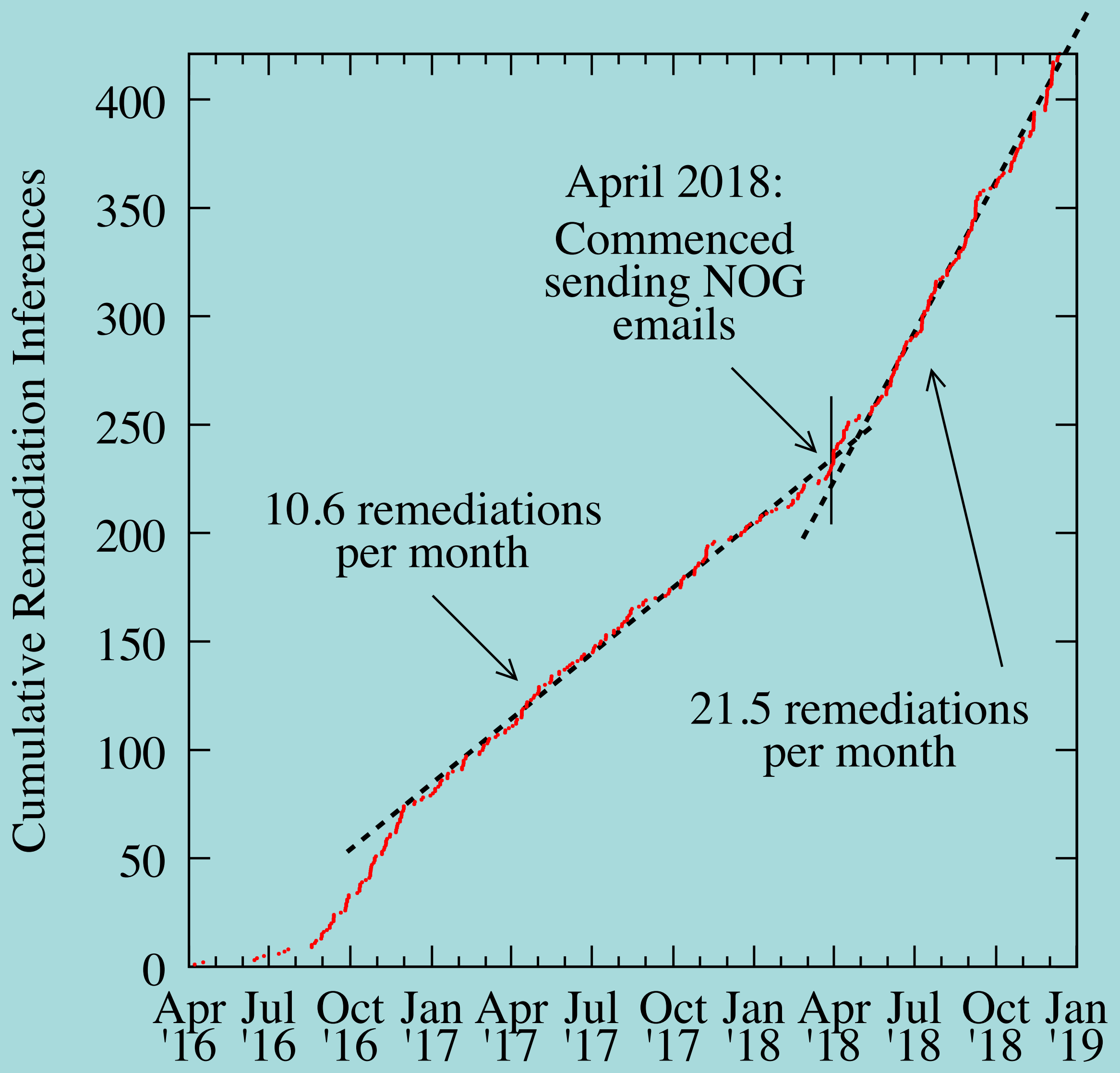


Attacker A is spoofing User U's address to send attack traffic to Victim V. Since V can not tell which packets really come from U, it is overwelmed by A's attack traffic, with no automated way to track this attack back to A.

OUTREACH & REMEDIATION

We perform outreach to ASes that our data indicates do not filter packets with spoofed source addresses. Until April 2018, our outreach was entirely private: we emailed the abuse or technical contact registered in WHOIS or PeeringDB of each AS.

Beginning April 2018, we also send monthly summary emails to region-focused network operator group mailing lists with summaries of ASes which, according to our data, have deployed SAV in the past month, or who do not block packets with spoofed source addresses. Outreach into the NOG community has resulted in doubling the number of networks deploying SAV per month in our data, from 10.6 to 21.5 per month.



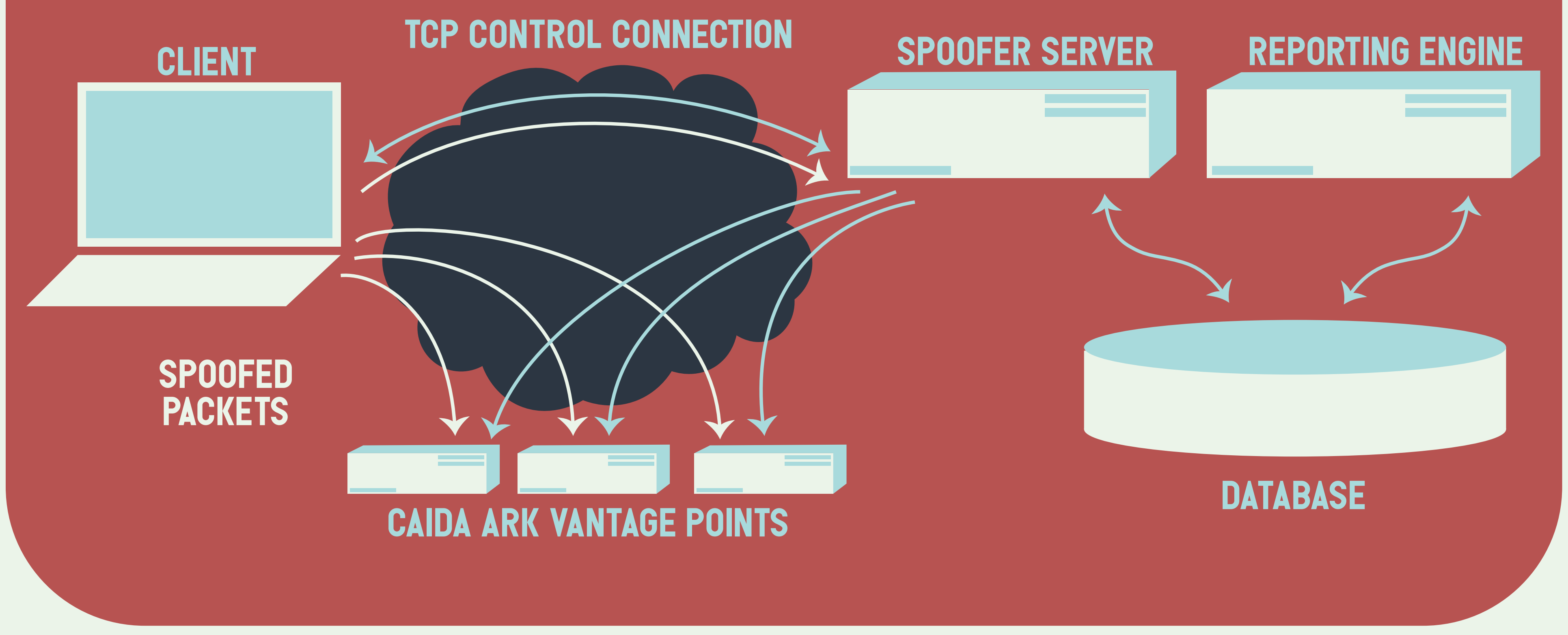
SOURCE ADDRESS VALIDATION ARCHITECTURE

In 2015, CAIDA, in collaboration with Matthew Luckie at the University of Waikato, released an upgraded version of Rob Beverly's original measurement system, with new and more robust measurement capabilities. The new client system provides several additional features:

1. *It runs in the background, automatically testing new IPv4 and IPv6 networks it attaches to, once per week.*
2. *The client includes a graphical user interface (GUI) to browse test results from your host, or schedule future tests.*
3. *How many addresses in larger prefixes containing that prefix can be spoofed. The Reporting Engine (spoofer.caida.org) publishes outcomes of sharable tests. By default the system publicly shares anonymized (to IPv4 /24 and IPv6 /40) results, and shares unanonymized results to authorized remediation personnel. Users can opt out of either type of sharing. The Reporting Engine accepts web queries of the resulting data, allowing users to select outcomes per country or ASN. To find out if your network provider(s), or any network you are using, allows IP spoofing, point your web browser at http://spoofer.caida.org and install the client software.*

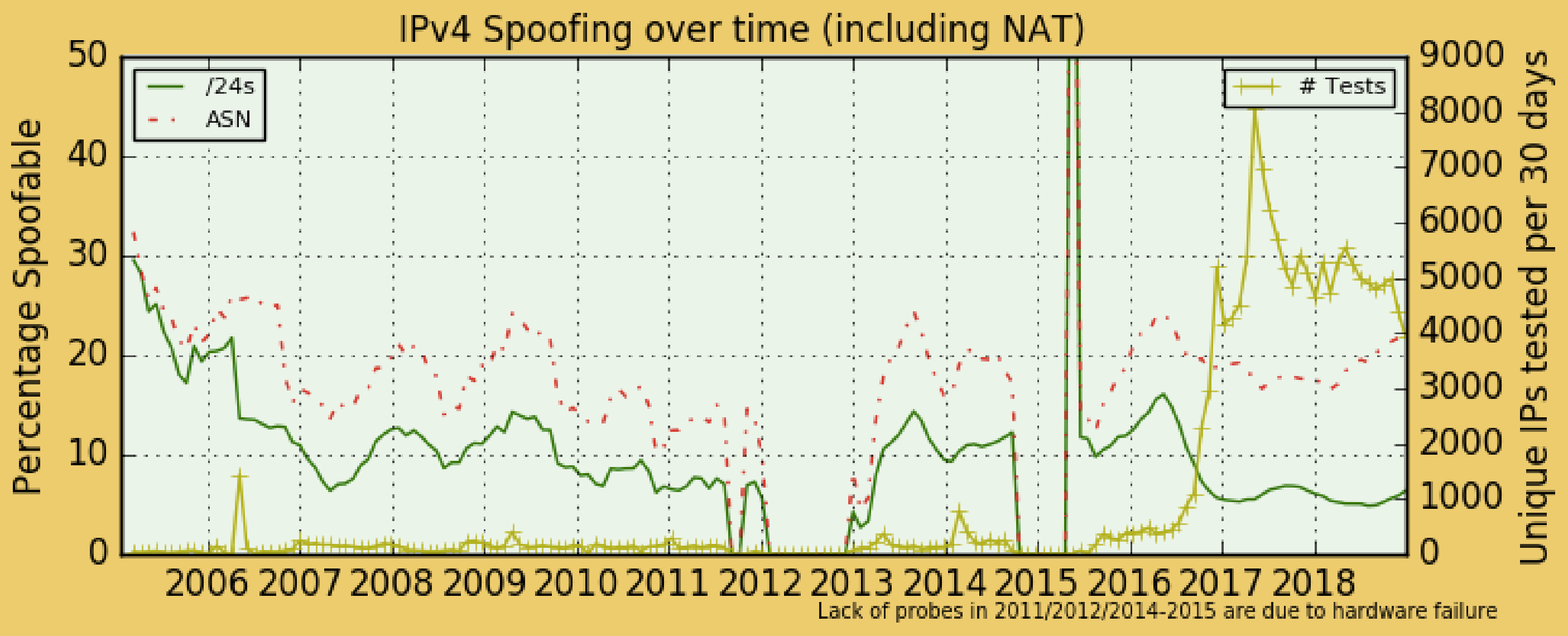
SPOOFER: CLIENT/SERVER OVERVIEW

The spoofer client sends a customized series of spoofed packets to the Spoofer server and CAIDA's Ark vantage points, as well as notifying the server what packets it sent. The server then compares the packets sent against those received and records this information into the database. The reporting engine supports querying of test results.

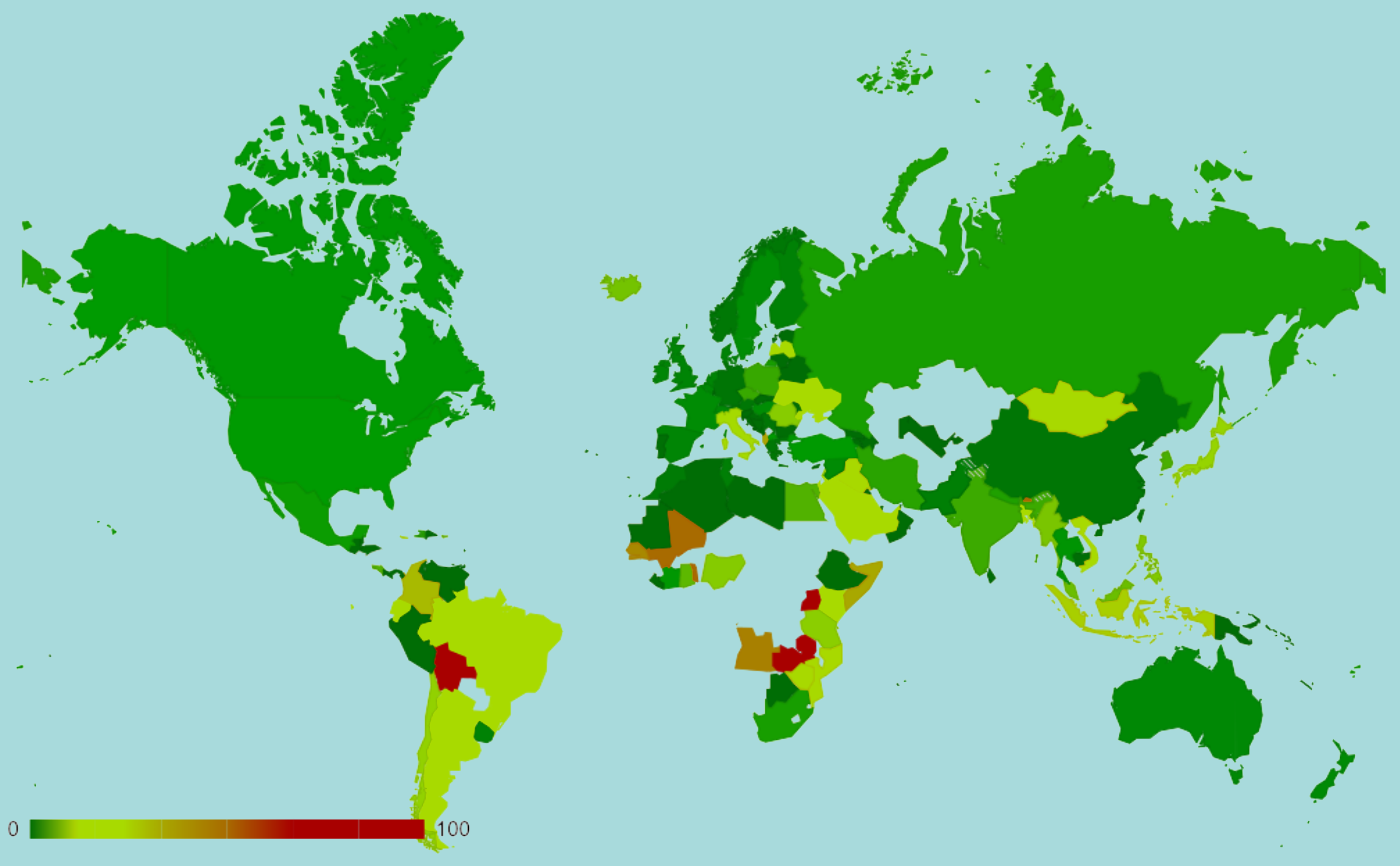


OBSERVABLE SPOOFABILITY OF PREFIXES, ADDRESS SPACE, AND ASES OVER TIME

To compensate for the sparse testing (and to prevent visual clutter), the spoofability calculation includes a 6-month window of tests before the specified date. Prefixes, addresses, or ASes with multiple tests with conflicting results are classified as spoofable.



PERCENTAGE OF TESTED IP BLOCKS SHOWING EVIDENCE OF SPOOFING



SPONSORS

This material is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division (DHS S&T/HSARPA/CSD) BAA HSHQDC-14-R-B0005, and the Government of United Kingdom of Great Britain and Northern Ireland via contract number D15PC00188. Views should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Department of Homeland Security, the U.S. Government, or the Government of United Kingdom of Great Britain and Northern Ireland.

U.S. DEPARTMENT OF HOMELAND SECURITY

caida

UC San Diego