Paper Review - S&P '15

Watch your Faultprints:
Secure Inter-domain Fault Localization

Shuai Hao

Dec. 2014

Proposed decision: Weak Accept (4 of scale 5)

Summary

Fault localization aims to enable the source to localize malicious entities on the network path in ISP/Enterprise network. Existing Fault localization protocols usually focus on the intra-domain setting and require the per-flow or per-source state installed at intermediate routers. Instead of installing states at routers, in proposed Faultprints protocol, each node on the network path performs a probabilistic sampling for the packets it forwards.

The probabilistic sampling hashes the data and acknowledgement packet and stores its fingerprint to a *Bloom Filter* (a multi-hash data structure indicating if a element is in the set) and thus requires only constant storage at each AS. At each epoch, an AS uses a sampling function produced by a secret key to determine sampling selection, and this secret parameter can be revealed to source to verify the sampling selection in next epoch. The inconsistent sampling behavior indicates suspicious entities on the network path. The Bloom Filter is flushed at beginning of each epoch to relieve the storage burden and the sampling key of each AS is updated at each epoch by driving a hash chain.

When the source does not receive a acknowledgement message from the destination, it sends (probabilistically) a probing message for the data packet. The destination and all ASes on the forward path need to response the probe with an anonymous reply, which indicates the Bloom Filter sampling state. The source calculates the *corruption scores*, according to the probing results showing the unexpected sampling behavior due to the malicious nodes, and the *misbehavior probability*, by accumulating the incorrect probe replies from each AS.

Comments

Foultprint relies on the time-synchronized nodes on the network path. In section of assumptions, the paper claimed NTP is used for loose-time synchronization. However, in section IV, ASes establish current epoch using source's timestamp attached by the packet. Since the protocol does not recognize the per-flow or per-source states, this statement is confusing. What if many sources with bad time-synchronization send the packets at one epoch? In section IV-A, the timestamp is only used to decide epoch the packet belongs to.

The proposed scheme requires a Faultprint router within each AS which is both on forward and return path. For the $\langle source, destination \rangle$ pair, an offline test is performed to validate the Faultprint router. 1) Does it means all the flow path need to be pre-examined before the Faultprint converges? 2) If a new

$\langle source, destination \rangle$ pair comes, how to ensure a Faultprint router is on the two-way path? 3) The paper also proposes ISPs adjust the BGP perimeters to ensure at least one router within each AS for some address subset is both on the forward/return path. Does this mean all traffic from this address subset will go through the specific router? It puts the high load on that device and introduces a single-point failure for the Faultprint protocol.

In section IV-A, the paper states "the source can probe for missing DACK packet in the same manner as probing for missing DATA packets". The statement is not accurate. I cannot see what's the difference between these two situations. The source performs the probing only because the DACK is missing. It cannot realize either DATA or DACK is dropped.

The example of Fig.3 is farfetched. It takes an assumption that the Faultprint router cannot be the adversary. With the untrustable hardware, a malicious node may be assigned as the Faultprint router that can easily know which packets it should be sampled and response a reply with valid value. Moreover, it can simply deny all sampling then the case 2 is meaningless.

The paper didn't present the handling for many corner cases. For example, malicious ASes will have more knowledge about the network path and may perform more sophisticated attacks if they are located at the ingress/egress of network path. Also, what if an AS drops all PReply messages? Since the source cannot tell whether the malicious AS also sends the PReply, all adjacent ASes become suspicious.

Pros and Cons

Pros

- The paper proposes a inter-domain fault localization protocol based on unpredictable committed deterministic sampling instead of installing per-flow or per-source state at intermediate routers. The usage of Bloom Filter storing packet's fingerprint provides an effective and efficient solution for sampling index.
- The evaluation is detailed and comprehensive.
- The paper is written and presented well.

Cons

- Although the system is designed to avoid storing per-flow state at intermediate nodes, all discussions (time-synchronizing, packet sampling) are based on a single-flow scenario.
- Since the paper assumed the node's hardware is not trustable, the routers could be able to perform more sophisticated attacks, e.g. fabricating a probing reply but with valid key. The example in the paper only presents some straightforward attacks and didn't demonstrate the availability and reliability of protocol when the hardware is compromised.
- The paper does not discuss whether the design works under the incremental deployment. If not, it becomes impractical in the common case.
- The proposed protocol works at AS-level. To enable the practical fault localization, an intra-domain protocol may still be needed, since circumventing an AS in common case is not easy even infeasible but circumventing a node is much easier.