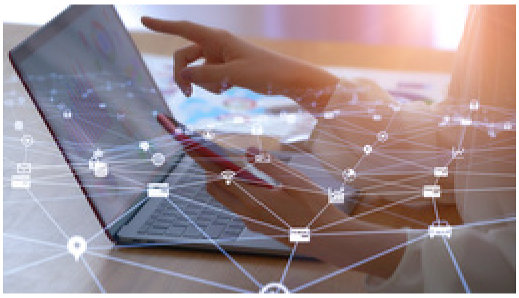
INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

Adaptive Network Probing Using Machine Learning

TECHNOLOGY NUMBER: 2020-516



OVERVIEW

Machine learning based framework for efficient probing of Internet hosts

- Uncovers 99% of active hosts for each probe at a low probing rate of 18.5%
- Enables users to identify malicious agents and vulnerabilities that are being actively exploited

BACKGROUND

Network scanning is widely used to assess security postures of hosts and networks, discover and examine vulnerabilities, and study trends in the Internet ecosystem. However, global scans of the IPv4 address space can generate large amounts of traffic for networks, especially when this is done by probing across multiple ports. For this reason, efficient probing of IPv6 hosts (where global scans are infeasible due to the exponentially larger address space) is an outstanding problem. This will become an increasingly critical issue as more hosts migrate to IPv6 and warrant representative measurements that can characterize hosts/networks in this space.

INNOVATION

Researchers at the University of Michigan have developed a machine learning based framework for the efficient probing of Internet hosts. This method is able to predict active hosts, which accelerates network scans, reduces the bandwidth of network scans, and ultimately promotes better Internet citizenship. To date, the researchers have been able to achieve very reliable predictions for discovering active IPs while guaranteeing consistent coverage, uncovering 99% of active hosts for each probe at a low probing rate of 18.5%. Moreover, they can significantly

Technology ID

2020-516

Category

Software

Software & Content

Inventor

Armin Sarabi

Kun Jin

Mingyan Liu

Tongxin Yin

Further information

Ashwathi Iyer

ashwathi@umich.edu

Learn more

reduce the bandwidth of scans over specific ports, probing less than 5% of all IPs for 24 probes, and less than 1% for 9 probes.

The University of Michigan researchers have also leveraged machine learning technologies, and more specifically deep reinforcement learning methods, to develop passive measurements of the Internet through the use of intelligent network honeypots. This method teaches a network honeypot agent how to respond to potential attackers who are probing a system in order to lure them into revealing their attack vector. This enables automated communication with Internet addresses that attempt to probe machines, hence collecting potentially malicious traffic for analysis by security researchers.

These active and passive measurements allow one to automatically and efficiently monitor the public Internet in order to reveal active Internet addresses, assess the attack surface of networks, and gauge the security of networks/hosts. Furthermore, it enables users to identify malicious agents, attack vectors, and vulnerabilities that are being actively exploited, and it provides more visibility into the Internet in a much less intrusive way than is currently being done.

PATENT APPLICATION

Number:Application number 63/105,492