Mapping Internet Sensors with Probe Response Attacks

Protecting Internet Sensor Anonymity

Jason Franklin

jfrankli@cs.wisc.edu

Department of Computer Science
University of Wisconsin, Madison

Outline

- The Case for Internet Sensors
  - Background
  - Governmental Initiatives
- Monitoring and Detection Systems
  - Currently Deployed Networks
  - Sensor Network Design
  - Utility vs Privacy
- Vulnerabilities in Internet Sensor Networks
  - Attacks on Sensor Networks
  - Probe Response Attack
- Countermeasures
  - Overview of Potential Countermeasures
- Conclusion
  - Review
  - Additional Resources

Definition

An Internet sensor network is a collection of systems which monitor the Internet and produce statistics related to Internet traffic patterns and anomalies.

They are useful for distributed intrusion detection and monitoring such as:

- quickly detecting outbreaks of worms and fast moving malicious code
- aggregating rare events from globally distributed monitors
- noticing attacks before the majority of vulnerable systems are compromised
- classifying the pervasiveness of threats like port scans, DoS attacks, and botnet activity

The National Strategy to Secure Cyberspace

- The *National Strategy to Secure Cyberspace* established a list of priorities, actions, and initiatives toward the development of a cyberspace monitoring infrastructure.

SECURE
CYBERSPACE

Priority I

"A National Cyberspace Security Response System"

Major Actions and Initiatives

- "Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace"
- "Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities"

Example Internet Sensor Network

infocon:GREEN
http://isc.sans.org

SANS Internet Storm Center

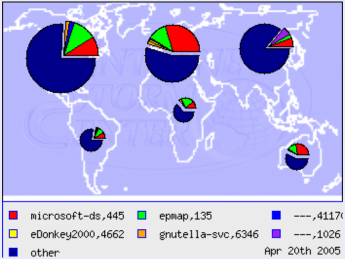
- collects firewall logs from over 650,000 IP addresses
- produces daily reports on Internet attack activity
- analyzes trends in traffic patterns to detect new vulnerabilities

The SANS Internet Storm Center, like other sensor networks, relies on individuals, corporations, and other administrative domains to share potentially sensitive information on Internet incidents.

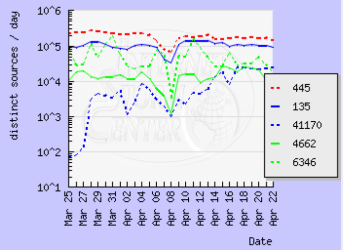
Internet Sensor Reporting Schemes

The SANS Internet Storm Center's global view and traffic graphs are representative of general Internet sensor reporting schemes.

Global View



Traffic Graphs



Sensor Network Design Considerations

For maximum effectiveness, an Internet sensor network must publish public real-time reports which the Internet community can then use to implement countermeasures.

Publishing Public Reports vs Keeping Information Private

- Public Reporting
  - Allows for a widespread response to cyber attacks
  - Facilitates information sharing involving cyber incidents
  - Increases the number of entities performing remediation and analysis activities
- Keeping Information Private
  - Satisfies privacy concerns of parties involved in cyber incidents
  - Allows for increased corporate and government participation
  - Limits the feedback attackers receive on the success of their attacks

Additional Sensor Network Design Considerations

Real-Time Reporting vs Delayed Reporting

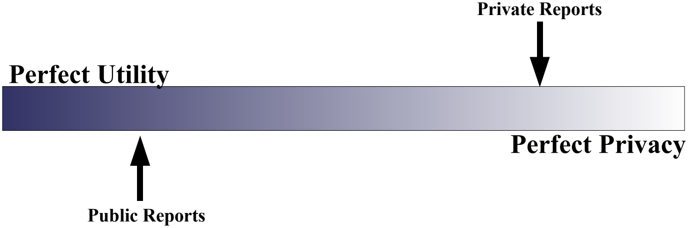
- Real-Time Reporting
  - Allows for an immediate response to rapid cyber attacks
  - Establishes a starting point for forensic analysis of compromised systems
- Delayed Reporting
  - Protects the privacy of parties involved by allowing for in depth anonymization
  - Provides for a strategic response to cyber attacks rather than a reactionary response

The Utility vs Privacy Tradeoff

- Internet sensor networks encounter the census problem.

Census Problem

Individuals give private information to a trusted individual (sensor network), who publishes a sanitized version of the data (reports). There are two fundamentally conflicting requirements, the **privacy** of the participant's information and the **utility** of the data.



Vulnerabilities in Internet Sensor Networks

The National Strategy to Secure Cyberspace

"... no cybersecurity plan can be impervious to concerted and intelligent attacks ..."

- Attacks on Internet sensor networks include:

Alert flooding	Overwhelming the network with false alerts
Data Poisoning	Skewing sensor statistics to hide malicious activity
Avoidance	Only targeting systems which are not sensors

- Each of these attacks assumes the ability to locate individual sensor's IP addresses. As a result, Internet sensor networks take steps to prevent the disclosure of sensor locations (IP addresses).

Mapping Internet Sensor Locations

- Internet sensor networks rely on the critical assumption that the set of sensor locations is secret.

Probe Response Attacks

Probe response attacks use intelligent probing to determine the locations of sensors.

General Attack Idea

Probe an IP address with activity that will be reported to the Internet sensor network if the address is among those monitored, then check the reports published by the network to see if the activity is reported. If the activity is reported, the host probed is submitting logs to the network.

Probe Response Algorithm

Our probe response algorithm relies on a divide and conqueror strategy to partition the Internet into **search intervals.**

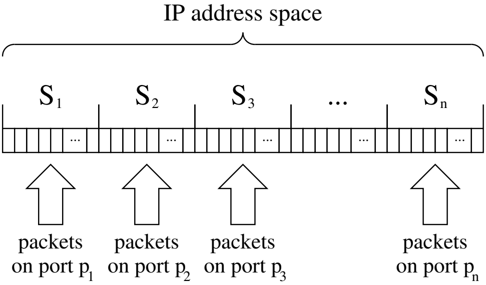
- The basic probe response algorithm operates in two stages.

  Stage I Probe the entire Internet to count the number of sensors in each search interval, S_i. Drop empty search intervals.

  Stage II Iteratively probe each remaining interval, R_i, until individual sensors are located.

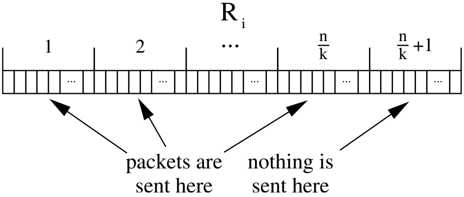
Stage I of the Probe Response Algorithm

In Stage I, we divide the Internet into search intervals, S_i, which are then probed for sensors. Search intervals with zero sensors are dropped.



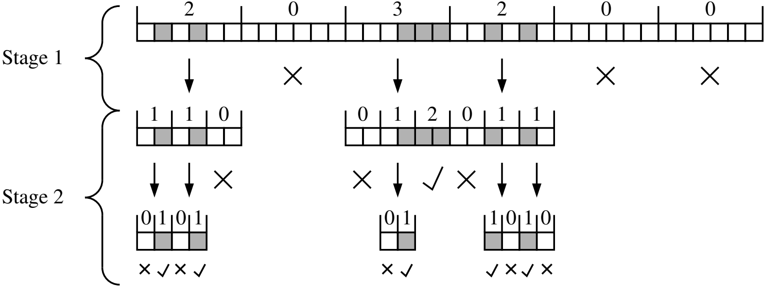
Stage II of the Probe Response Algorithm

In Stage II, we take each remaining interval, R_i, and continue an iterated probing process until individual sensors are located.



Probe Response Attack Illustration

A simple example probe response attack consisting of Stage I and two iterations of Stage II.



Defending Against Probe Response Attacks

Problem

How do we prevent probe response attacks from locating Internet sensors while maintaining public real-time reports?

Solution

We use a combination of defenses which seek to slow the attacker and decrease the probability of an error free mapping.

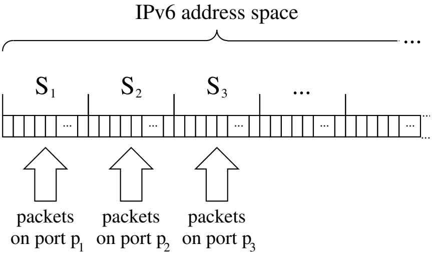
Defending Against Probe Response Attacks

Defenses include:

Scan prevention	Stops an attack at Stage I
Sampling	Corrupts the probe responses in both stages
Limited reporting	Reduces the effectiveness of each stage
Delayed reporting	Slows down each stage of the attack

Scan Prevention Explained

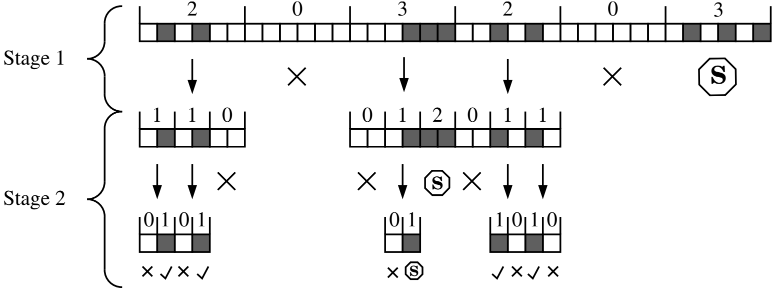
- Usage of IPv6
  - Increases the number of IP addresses to scan from around 2^{32} to 2^{128}
  - Prevents Stage I of the attack from completing in a reasonable amount of time
  - Allows Internet sensors to hide amongst a sea of IP addresses



Sampling Explained

- Sampling corrupts the results of both stages of the attack by eliminating responses to particular probes.

Below we illustrate an example of sampling.



Pros and Cons of Limited Reporting

Definition

Limited reporting is the concept of minimizing the number of reports available to an attacker.

Limited Reporting

- Pros:
  - Reduces the number of probes which can be used to locate sensors
  - Slows the progress of both Stage I and Stage II of the attack
- Cons:
  - Reduces the utility of the Internet sensor network's data
  - May not completely prevent probe response attacks

Pros and Cons of Delayed Reporting

Definition

Delayed reporting is the process of retaining reports for a specified period of time before release.

Delayed Reporting

- Pros:
  - Reduces the rate at which probe responses can be received
  - Slows the progress of an attack by a specified amount
- Cons:
  - Violates our central requirement of a real-time reporting system
  - Internet sensor networks may still be vulnerable to a nonadaptive probe response algorithm

Key Points to Remember

- Internet sensor networks are systems which monitor the health of the Internet.
- The *National Strategy to Secure Cyberspace* dictates guidelines for the creation of an Internet sensor network.
- A number of attacks on Internet sensor networks rely on the ability to locate individual sensors.
- Probe response attacks can be used to quickly and efficiently locate Internet sensors.
- Scan prevention, sampling, and limited and delayed reporting are effective countermeasures against probe response attacks.

Final Advice

Internet sensor networks should be designed to resist probe response attacks.

Resources for Further Information

USENIX Security '05	"Mapping Internet Sensors with Probe Response Attacks" by John Bethencourt, Jason Franklin, and Mary Vernon.
CIPART Project	http://www.cs.wisc.edu/∼vernon/cipart.html
Web Page	http://www.cs.wisc.edu/∼jfrankli

Coauthor Information

- John Bethencourt

  Affiliation: University of Wisconsin, Madison
  Email: bethenco@cs.wisc.edu

- Professor Mary Vernon

  Affiliation: University of Wisconsin, Madison
  Email: vernon@cs.wisc.edu

Jason Franklin

Picture

Contact Information

Email: jfrankli@cs.wisc.edu
Web: http://www.cs.wisc.edu/∼jfrankli

Biographical Note

Jason Franklin graduated from the University of Wisconsin, Madison with a B.S. in computer science and mathematics. He won a Department of Homeland Security Scholarship in 2003 and is currently a Ph.D. student at Carnegie Mellon University.