Topological Models and Effectiveness of Network Telescopes

This thesis will look at Darknets or Internet Sinks and their ability to predict network attacks.

BY FOTIS GAGADIS AND STEPHEN D. WOLTHUSEN

Royal Holloway
University of London

UNDERSTANDING DoS ATTACKS THROUGH UNUSED IP ADDRESSES

Network attacks, particularly denial of service (DoS) style attacks and rapid propagation malware such as worms, remain a considerable threat whose severity is exacerbated by the very presence of high-speed networks. The low latency and high bandwidth of such networks facilitates extremely rapid attack patterns and worm propagation, leaving very little time for active countermeasures. It is therefore imperative to obtain as much early warning information as possible to assist in setting up or configuring appropriate defensive mechanisms.

Moore et al., from the Cooperative Association for Internet Data Analysis (CAIDA), have recently proposed a measurement and monitoring method for networks and the Internet which make use of the fact that attackers may inadvertently target non-existent areas of the Internet address range and use spoofed source addresses, which can also result in traffic being sent to non-existent addresses. This method of monitoring and measurement is called network telescopes.

In analogy to their optical equivalent, network telescopes detect malicious behaviour by observing small, unusual phenomena that occur in dark places. For the network telescope, these are the unused network address in a network. Any data received by an unused network address must be the result of denial of service attacks, worm propagation, or misconfiguration. In this article, we will briefly discuss the nature of network telescopes' underlying topological models and their effectiveness.

Fotis Gagadis
Royal Holloway, University of London
Information Security Group
fgagadis@yahoo.gr

Stephen D. Wolthusen
Royal Holloway, University of London
Information Security Group
stephen.wolthusen@hig.no

This article was prepared by students and staff involved with the award-winning M.Sc. in Information Security offered by the Information Security Group at Royal Holloway, University of London. The student was judged to have produced an outstanding M.Sc. thesis on a business-related topic. The full thesis is available as a technical report on the Royal Holloway website http://www.ma.rhul.ac.uk/tech.

For more information about the Information Security Group at Royal Holloway or on the M.Sc. in Information Security, please visit http://www.isg.rhul.ac.uk.

Topological Models and Effectiveness of Network Telescopes

1 INTRODUCTION

Recently, researchers at CAIDA proposed a system that is able to monitor pandemic and endemic incidents, such as worms or denial of service (DoS) attacks, through the use of unused (dark) IP addresses. These efficient systems, called network telescopes, have the ability to monitor and characterize malicious phenomena through specialized mathematical tools, sensors and virtual machines.

The topological models are designed to offer efficiency and monitoring effectiveness of so-called dark addresses activity in a network. This use of unused (dark) addresses help the network telescope to efficiently monitor unsolicited traffic, propagation and misconfiguration since the activity arriving in those ranges can be assumed to be a result of malicious activity or problems in a network.

Moore et al. proposed network telescopes as an alternative to existing network and security monitoring and measurement systems. Network telescopes are currently used mostly for academic purposes and gathering data on distributed topologies for Internet observations. As previously mentioned, a network telescope observes a portion of routed IP addresses where no or little legitimate traffic exists.

Therefore, any traffic seen by the telescope must be the result of misconfiguration, worms scanning or backscatter traffic from spoofed addresses [7]. Network telescopes are sometimes called Darknets, BlackHoles, or Internet Sinks [1].

It must be noted that a network telescope's monitoring ability is proportional to the packets received by randomly selected IP addresses, the size of the address space monitored, and to the number of distinct incidents observed [9]. While the majority of network telescopes passively monitor traffic, there are also advanced telescopes that could perform active monitoring [3].

Conceptually, network telescopes are analogous to astronomical telescopes. In this analogy, having a large address space is equivalent to a larger or more sensitive sensor for photons arriving at the telescope, resulting in a higher probability for the telescope to observe certain phenomena. Through this analogy, a network telescope observing a large IP address space has a greater probability of observing a security incident and will collect more data for further analysis. While observing a large fraction of IP addresses, the ability of the telescope to monitor traffic flow, categorize the features of any activity, and eventually to characterize the phenomena, is higher [12].

This article will explain the topological models of network telescopes. Moreover, there will be an analysis on the efficiency

While the majority of network telescopes passively monitor traffic, there are also advanced telescopes that could perform active monitoring [3].

of network telescopes and the advantages/disadvantages of the different topologies.

IP (Internet Protocol) IP is one of the most important protocols from the TCP/IP suite. IPv4 addresses are logical addresses consisting of 32 bits and have 256 possible combinations, however 0 represents the local address and 255 the broadcast address. Therefore, the real range IP addresses are from 1 to 254 for network hosts. A part of the address is assigned to the network and part to the host.

For instance, the 172.24.206.18 IP address has a network identity of 172.24.0.0 and a host identity 206.18 [17]. The purpose of this section is not to introduce IP addressing but to briefly describe classes and prefixes of networks, to allow the reader to understand network telescopes.

Today, the networking community makes use of the Classless InterDomain Routing (CIDR) system.

The CIDR makes use of notations like /x to describe the network's prefix. We will briefly explain the IP class system only for reader's information and for the purposes of efficient reading. There are five IP classes in total. Class A addresses are intended for large numbers of hosts and especially large corporations. Class A addresses have a network identity from 1 to 126, and allow 16,777,214 hosts per network. Class B addresses range are from 128-191 and allow 65,534 hosts per network. Class C range from 192 to 223 and allows 254 host per network. Class D is used for multicasting purposes and has a range of 224-239. Class E has a range of 240-255 and is used for experimental reasons mostly [17].

So, the number of possible addresses is 2^{32}. A /8 (Class A) network has range of 2^{24} addresses which have in common the first 8 bits. The /16 (Class B) network, has range of 2^{16} addresses which have in common the first 16 bits. A /24 (Class C) network has 2^{8} addresses which have in common the first 24 bits. Thus, a /32 address is a unique IP address [12]. The notation /x will be used later on this article.

2 MODELS OF NETWORK TELESCOPES

There are two general topological models characterizing the functionality of network telescopes. A passive telescope observes the packets arriving, keeps logs and later discards them without further interactions with the attacker [4, 16]. By this interactivity,

IP (Internet Protocol) IP is one of the most important protocols from the TCP/IP suite.

the passive telescope will observe hosts and packet information, but no further information will be captured about an attack or misconfiguration.

For instance, a TCP handshake will be monitored as an attempt to initiate a connection [7]. The headers and payloads observed can be analyzed offline for the characterization of incidents and there will be an extended analysis on protocols, sources, type, ports and destinations attacked, but a passive telescope cannot identify attacks before malicious activity [4]. Passive telescopes, consequently, are especially useful for measuring attacking behaviours of pandemic incidents (i.e worms) [18].

Active telescopes, on the other hand, respond to incoming packets and establish communication channels until the incident is identified. A telescope of this type emulates services, distinguishes/analyzes attacks and keeps tracks of the attacker. Contrary to passive telescopes, an active telescope is resource-intensive and it is crucial for the administrator to decide the active responder's type (i.e the responder might be a sensor or a specific device that responds to the packets arriving at the telescope). The active response might be either stateful or stateless. A stateful responder will retain each connection's state if it is active. A stateless responder will design a response based on received packets [4]. By responding to the incoming traffic, an active telescope will collect more information about the incident than a passive telescopy. On the other hand, if the interaction with the telescope means that the attacker can identify the address space monitored by the telescope, then it can avoid further interaction with the telescope [7].

2.1 Distributed Network Telescope

A distributed network telescope is the combination of several smaller telescopes into a much larger one. This distributed telescope can monitor a much bigger addresses range, which can take the form of contiguous ranges such as heterogeneous distributed systems and P2P networks [12]. This topology has the characteristics of passive models and it is highly regarded for its measuring capability on pandemic incidents [18].

The Internet Motion Sensor (IMS) is based on the theory of distributed telescopes. IMS's ability to detect malicious phenomena extends from /24 distributed nets over the globe [5] and consists of 60

A distributed network telescope is the combination of several smaller telescopes into a much larger one.

telescopes from 18 organizations, enterprises and academic networks in three continents. The IMS monitors approximately 17 million addresses and over 2.5 years received an average of 9 packets/second [7]. In addition to its characteristics, IMS provides wider visibility and has the ability to differentiate/ characterize traffic. Furthermore, it supports real time trending and data analysis. On the other hand, because of the large collection of data, if this data is not properly processed, then the system may report a large number of false positives or false negatives. Since the amount of data that IMS collects is so large, processing the data can be a problem. This data processing is done by the sensors themselves, rather than by a central database, to keep the data processing phase efficient. The sensor stores MD5 checksums and compares them with the data arriving. If a new checksum is found, the MD5 checksum is stored for future comparison [2].

2.2 Anycast Network Telescope

Anycast telescopes make use of multiple locations for the proper advertisement of routes at the same /x network and do not monitor large ranges of addresses such as a distributed telescope. By advertising /x prefixed locations, the telescope provides efficient monitoring of events. This event flow will be smaller, generally, because of the hosts' locations and of the telescope's monitoring in a /x network. A telescope of this category, consequently, will distribute flow, load, traffic over many locations resulting in an event flow observance faster than other topologies [12]. McPherson et al. suggest that anycast telescopes can effectively distribute, manage and discard packets. Anycast telescope will discard packets if they do not have any specific further uses (i.e analysis of recorded data) [8].

2.3 Transit Network Telescope

Moore et al., according to their technical report for network telescopes, describe a transit network telescope which monitors IP ranges, but from within the transit network and not from the edges of the /x network. This kind of architecture observes large ranges of addresses, manages to monitor centrally and does not have synchronization/distribution problems. A telescope of this category can only effectively monitor IPs from the same network. However, accurately characterizing events is not efficient with a

Since the amount of data that IMS collects is so large, processing the data can be a problem.

transit telescope. A transit telescope, consequently, is efficient for the detection of events, but cannot characterize events in detail. For instance, the transit telescope cannot describe the headers of the packets in detail like a distributed system [12].

2.4 Honeyfarm

An example of an active topology is the honeyfarm telescope. A honeyfarm telescope actively responds to the traffic. The range of monitored addresses must be decided by the administrator. Moreover, since many events will occur at the same time (i.e active responses), depending always on the prefix monitored (e.g a /8 prefix is 16 million addresses), there will be a high rate of events and the traffic can be intermixed with insignificant background traffic. Therefore, the amount of active responses must be carefully decided, from honeyfarm point of view, because they can overload the system [12].

A honeyfarm is a collection of honeypots monitored by a network telescope and any outgoing traffic from a honeyfarm will be an activity from a pandemic incident [13]. Some researchers make use of honeynets, instead of honeypots. Honeynets which are highly interactive honeypot systems. The honeynet can provide applications, services and emulation of operating systems such as Solaris, an internet site or VAX systems [14]. An example of this category is the Collapsar, a system with highly-interactive virtual honeypots which are located in a local network. The honeypots of this system are configurable, manageable, easily monitored and have the ability to detect/stop various incidents [6].

2.5 Greynets

Harrop et al. proposed Greynet as a network telescope. A greynet consists of unused IPs and assigned ones. The network is sparsely populated with unused IPs interspersed between active addresses for effective traffic monitoring. The active IPs are assigned to hosts on the network and by interspersing unused IPs among active ones, there is higher probability for the network telescope to observe a phenomenon such as a malware attack [5].

3 EFFECTIVENESS OF NETWORK TELESCOPES

A network telescope makes use of dark (unused) IPs and no legitimate traffic should exist in the monitored space. Since no legitimate traffic exists in the monitoring space,

A network-based detection system, which can be even based on simple traffic analysis, could detect suspicious values in the different certificate fields used by the attacker (i.e. strange serial numbers).

the resulted activity must be from misconfiguration, backscatter activity, worm propagation or other type of network probing [7].

Telescopes, moreover, can effectively observe large explosions of incidents, but its effectiveness depends on proper statistical/mathematical tools [9]. Interestingly small telescopes sometimes receive more packets/day than larger ones. Typically a /24 has a rate of 9 packets/second, a /16 has 75 packets/second and a /8 telescope monitors approximately 5,000 packets/second [7]. Since short and low intensity attacks generate less packets, a larger monitoring space is required to resolve any information from the monitored activity [11].

Furthermore, researchers observed that addresses generating data for a telescope had differences in magnitude. Consequently, there must be a mechanism in order to check if the data is manageable and can be generalized for further analysis. For instance, if the network sensors are under DoS attack, the incident could cause congestion and overloading of the network. Hence, the visibility of the telescope and the traffic analysis is affected. Statistical differences, moreover, arise from the sampling traffic and therefore the results are different in every monitor. Thus, hypothesis testing for homogeneity must be used to resolve further issues [2].

Moore et al., additionally, explained that while selecting an address range for a telescope, there are a variety of reasons that IPs must be randomly and uniformly selected. For example, there may be a bias in activity in some regions. For instance, worms spread with the use of nearby addresses and if the propagation acts in a non-selected range, the activity will not be monitored. These biases may affect the effectiveness of a telescope and results generated from an analysis [12].

There must be a consideration of the recorded events: e.g. how they are stored. Moreover, the data collection and analysis systems might have limitations to their capacity and processing capabilities.

Therefore, in the case of an aggressive event at its peak, the storage and processing systems might collapse. Additionally, routing instabilities affect the results observed through a network telescope and traffic data might be lost resulting in deficient analysis and classification of data. One of the solutions considered to the above problems is the distributed telescope [12].

Telescopes, moreover, can effectively observe large explosions of incidents, but its effectiveness depends on proper statistical/mathematical tools [9].

Furthermore, according to [15], a network telescope must be able to survive an incident or attack itself. Moreover, a network telescope must not trigger false alarms and telescope's architecture must be safe from the attackers. If the telescope's architecture is not under control of the administrator and the architecture is exposed to third persons, the worm architect can create pandemic phenomena which can avoid the sensors of network telescopes. Therefore, the deployment of telescope sensors must be under control of the administrator, the worm architect must not know the location of telescope's sensors, and the attackers must not control the telescope's sensors.

4 CONCLUSION

Network telescopes are effective tools for observing large-scale events based on mathematical models [9] and requiring careful observations, but they potentially provide early warnings of events that otherwise would be very difficult to obtain [2]. In deploying network telescopes, however, administrators and researchers must consider the various constraints of a network. Because of the sensitivity to telescope topology, it is also necessary to perform homogeneity tests to ensure results are not skewed inadvertently [2] and telescopes must monitor a randomly selected IP range or else they might not have the opportunity to observe pandemic incidents [12].

Topology is a key characteristic for the abilities and sensitivity of network telescopes. For instance, when placing a network telescope behind a security device, it clearly might not be able to observe part of the traffic resulting in false conclusions [7]. Given the scale of networks requiring observations, storage and collection also become an issue. Data rates can easily surpass 30G/day and the administrator must decide the type of services running on the topology for effective monitoring and reaction [7, 10]. Consequently, network telescopes are a delicate security technology which must be carefully placed and administered. However, a network telescope topology has the ability to monitor crucial phenomena and may provide the only warning capability available for critical services and networks.

Ron Condon

UK bureau chief
searchsecurity.co.UK

Ron Condon has been writing about developments in the IT industry for more than 30 years. In that time, he has charted the evolution from big mainframes, to minicomputers and PCs in the 1980s, and the rise of the Internet over the last decade or so. In recent years he has specialized in information security. He has edited daily, weekly and monthly publications, and has written for national and regional newspapers, in Europe and the U.S.

REFERENCES

[1] L. Andersson and L. Zhang, Report from the iab workshop on unwanted traffic march 9-10, 2006 draft-iab-iwout-report-00.txt, Tech. report, Network Working Group, Internet-Draft IETF, March 2006.

[2] Evan Cooke, Michael Bailey, Z. Morley Mao, David Watson, Farnam Jahanian, and Danny McPherson, Toward understanding distributed blackhole placement, WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode (New York, NY, USA), ACM Press, 2004, pp. 54–64.

[3] Jerome Francois, Radu State, and Olivier Festor, Tracking global wide configuration errors, Tech. report, Management of Dynamic Networks and Services Laboratoire Lorrain d'Informatique et des Applications de Lorraine Nancy, France, 2006.

[4] Julia Grace and Claire OShea, Network telescopes.

[5] Warren Harrop and Grenville Armitage, Greynets: A definition and evaluation of sparsely populated darknets, August 22-26 2005, Centre for Advanced Internet Architectures, Swinburne University of Technology Melbourne, Australia.
5

[6] Xuxian Jiang and Dongyan Xu, Col lapsar: A vm-based architecture for network attack detention center, Tech. report, USENIX, August 9-13 2004.

[7] Bailey M., Cooke E., Jahanian F., Myrick A., and Sinha S., Practical darknet measurement, Information Sciences and Systems, 2006 40th Annual Conference on, no. 10.1109/CISS.2006.286376, March 2006, pp. 1496 – 1501.

[8] Danny McPherson and Barry Greene, Isp security: Deploying and using sinkholes, June 2003.

[9] David Moore, Network telescopes overview: What is a "network telescope"?, 2003.

[10] David Moore and Colleen Shannon, Network telescopes: The flocon files, 2004.

[11] David Moore, Colleen Shannon, Douglas J. Brown, Geoffrey M. Voelker, and Stefan Savage, Inferring internet denial-of-service activity, Tech. Report 2, ACM, New York, NY, USA, 2006.

[12] David Moore, Colleen Shannon, Geoffrey M. Voelkery, and Stefan Savagey, Network telescopes: Technical report,

Tech. report, Cooperative Association for Internet Data Analysis (CAIDA), July 2004.

[13] Vern Paxson, Addressing the threat of internet worms, ICSI Center for Internet Research and Lawrence Berkeley National Laboratory, Feb 2005.

[14] Honeynet Pro ject, Know your enemy: Honeynets, Nov 2002.

[15] Joel Sandin, P2p systems for worm detection,dimacs large scale attacks workshop presentation, DIMACS Large Scale Attacks Workshop presentation, Sept 2003,.

[16] Christian Seifert and Ian Welch and Peter Komisarczuk, Taxonomy of honeypots, Tech. report, Victoria University of Wellington. Te Whare Wanangaote Upokoote Ikaa Maui, June 2006, TechnicalReportCS-TR-06/12.

[17] Greg Tomsho, Ed Tittel, and David Johnson, Guide to networking essentials, ed 3rd ed., Course Technology, no. ISBN: 0619130873, Thomson, 25 Thomson Place, Boston, Massachusetts, 02210, 2003.

[18] Yegneswaran Vinod, Barford Paul, and Ullrich Johannes, Internet intrusions: Global characteristics and prevalence, Tech. report, In Proceedings of ACM SIGMETRICS, June, 2003.