Mohonk: Mobile honeypots to trace unwanted traffic early

Balachander Krishnamurthy
AT&T Labs–Research
bala@research.att.com

Honeypots have been traditionally used to advertise dark address space and gather information about originators of traffic to such addresses. With simple thresholding mechanisms this technique has shown itself to be fairly effective in identifying suspicious IP addresses. Honeypots are however unsuitable to locate the precise entry point of unwanted traffic. Tracing back to the origination of such traffic is hard due to the delay and difficulty of maintaining state along the path of such traffic. We propose a novel mobile honeypot mechanism that allows unwanted traffic to be detected significantly closer to the origin. The mobility in our scheme stems from additional information that is made available to the upstream ASes as well as the changes in the set of dark address space advertised. Sharing information with a network of friendly ASes has the potential to identify and significantly lower unwanted traffic on such links.

Categories and Subject Descriptors

C.2.3 [**Network operations**]: Network monitoring

General Terms

Security,measurement

Keywords

unwanted packets, network monitoring

1. INTRODUCTION

There have been several attempts to identify originators of attack packets on the network. A common technique is a *honeypot* mechanism and is defined broadly as a *resource whose value lies in its unauthorized use* [1, 2]. Simple honeypot mechanisms involve advertising *dark address space* (a set of IP addresses that are not currently in use; i.e., associated with active machines) and identify originators of traffic to that space. The assumption is that such sources are suspicious. Some honeypots listen passively to such traffic. Neither the advertisements of dark prefixes nor the passive listening to incoming traffic is particularly expensive. Other honeypots interact with the traffic to varying degrees. Some respond with SYN-ACKs to the incoming SYNs or emulate a login session. At the other extreme, some honeypots may emulate a whole kernel. Depending on the degree of interaction more details about the attack traffic can be gathered. A network *telescope* [3] provides the ability to see victims of certain kinds of denial of service attacks or hosts infected by worms, and misconfigurations from a distance. Tarpits [4] have been deployed to waste resources of suspicious attack sources[1]. Honeypots can help identify suspicious IP addresses [5]. Public domain versions of honeypot code for popular operating systems have been available for different variants of probing attacks [6] along with commercial software [7] indicating the popularity of this technique for identifying probe traffic. The broad notion of honeypots has even been used to locate spam email originators [8] although such honeypots need to have more infrastructure in place.

Since honeypots gather data at the destination of probing and other unwanted traffic, they are unable to locate the precise entry point of such traffic; additionally some of the source addresses may be spoofed. Traceback to the origination of such traffic is hard due to the delay and difficulty of maintaining state along the path of such traffic. Most importantly, the ASes in the path towards the destination are not aware that the advertised prefix is dark. Thus, the ASes in the path carry such traffic towards the destination and are unable to benefit from the knowledge that the originators of such traffic are potentially suspect. Finally, the AS at which such traffic originated cannot learn about the link responsible for injecting this traffic.

In this paper we restrict the use of the term honeypots to entities that advertise dark prefixes for the purpose of identifying sources of unwanted packets and take one of a few actions.

To share the information about dark prefixes to upstream ASes, we propose *mobile honeypots* with a goal of detecting unwanted traffic significantly closer to the origin. The *mobility* stems from two aspects: the *information* about the darkness of the prefixes is made available to the upstream ASes. The mobility of this information enables multiple participants to be aware of attack sources earlier. The list of dark prefixes can be changed aperiodically and thus from the attackers viewpoint the honeypots appear to be mobile.

The mobile honeypot technique is proposed as a *low cost*, *reliable* mechanism that cannot be easily reverse engineered

[1]Questions about the legality of tarpits have been raised.

SIGCOMM'04 Workshops, Aug. 30+Sept. 3, 2004, Portland, Oregon, USA.

or attacked easily by malicious entities on the net. A key goal is to dynamically share the information gleaned with a network of friendly ASes. Each AS that learns about prefixes responsible for generating significant amounts of unwanted traffic are free to take remedial action. For example, if the ASes along the path know that the destination towards which traffic is being carried is a honeypot, they can drop such traffic and simply inform downstream ASes about these addresses using out of band mechanisms (e.g., as proposed in [9]).

What would be the motivation for ASes to cooperate in such a mechanism? Information about sources that are generating significant amount of probing or other traffic can be used by any of the ASes along the path. They could decide to graylist or drop *all* traffic from these sources when they are destined to their customers. Source-based filtering is typically not done as it carries a higher risk. However, as information about repeated probings spread, the source information can be selectively used by ASes along the path to influence their policies. Each of the ASes cooperating in the scheme can optionally augment the advertisements of dark prefixes. As each co-operating AS filters out traffic at the earliest possible upstream location and passes on the information about source IP addresses, there is potential reduction of unwanted traffic entering the Internet through any of the cooperating network of ASes.

The rest of the paper is as follows: the operational details of mobile honeypots is described in Section 2 and Section 3 discusses Mohonk's current implementation status. Section 4 examines a variety of possible attacks against the Mohonk scheme and Section 5 examines related work. We conclude with ongoing and future work in Section 6.

2. OPERATING MOBILE HONEYPOTS

Our proposal is for one or more ASes to choose a set of dark prefixes, advertise them for a certain duration and gather information about any packets that are sent to that destination. In this sense, it resembles a standard honeypot. As mentioned earlier, the mobility in our honeypots refers to the movement of *information* associated with dark prefixes as well as the changes in the set of dark prefixes advertised. There are three parameters an AS participating in the Mohonk scheme would use to tailor the operation:

- Prefixes of various lengths
- Duration of advertisement
- Threshold of packet count

Each AS selects at random from within its supernet, a varying subset of dark prefixes of differing lengths (say, a /24 typically) and advertises them. The advertisement is withdrawn after a certain random duration subject to some minimum and maximum time period limits. Along with the prefix and varying with the length, a threshold count of packets is identified: if the number of packets received at that destination exceeds that threshold within the duration of advertisement, then the originator is deemed as suspicious. This is to get around the somewhat benign probing associated with discovery of new prefixes (by Internet mapping entities and researchers). The algorithm for choosing prefixes, their liveness duration, and the count threshold are all independently determined by the participating ASes based on their traffic patterns and expected number of packets within a time interval. Along with the advertisement an optional field is used to enable the upstream AS to drop the traffic but pass on the information about the originator. We will explore actual BGP mechanisms to do this later in the paper.

How are dark addresses chosen? We can use synthetic models (such as AAWP [10]) which helps identify the number of addresses that can be used as honeypot sources. The goals of selecting addresses are multiple:

1. The attackers should be able to reach one of the selected addresses (i.e., the honeypot must attract a few bees) within the live duration of the prefix. The set of addresses should be large enough but presumably not too large to reduce false positives.

2. The non-cooperating ASes (or even co-operating ASes) should not be able to infer anything significant from the dark prefixes announced. ASes are concerned about this due to business and competitive reasons. Since an AS is free to withdraw the announcement of a dark prefix and assign it to a customer at any point in time in the future, the ASes that saw the fake announcements will not be able to infer anything of value from them.

3. If a dark address space is later assigned to valid customers, there should be little risk of traffic being dropped by upstream ASes.

Cooperative and non-cooperative operations: We envision two modes of operation for mobile honeypots: non-cooperative and co-operative. In the non-cooperative mode of operation, the announcing AS does not have to inform upstream ASes that a particular prefix is dark. A standard BGP announcement about a prefix is used and withdrawn after a certain duration. An internal threshold is used to conclude that when traffic for the prefix exceeds the threshold, the originator of such traffic is involved in sending spurious packets. In the non-cooperative mode, the unwanted traffic is carried all the way back to the announcer of the advertisement. The information about the originator can only be shared later with others in the path.

In the co-operative, and preferred form of operation, interested ASes add a tag in the community parameter in the BGP advertisement, so that the upstream ASes are aware of the dark nature of the prefix. Upstream ASes filter traffic directed towards these dark prefixes in one of two ways: they can identify the traffic, record the information and pass it on. Alternately they could *drop* the traffic but log the information and send it using out of band mechanisms [9] to the cooperating set of ASes.

How much additional work is required of a AS? In the non-cooperative mode the non-participating ASes accept updates (advertisements and withdrawals) on existing BGP connections and carry any traffic destined towards these prefixes. The volume of such traffic is not likely to be too high for them to be adversely affected and examining the economics of settlements, there is no potential downside. In the co-operative mode, whereby ASes actually know in advance that traffic destined towards the dark prefixes is unwanted, they can record the originator and then filter such traffic. Co-operating ASes would have to start maintaining additional checks for traffic towards a collection of prefixes ex-

ceeding specified threshold during the live window. Once they have learnt about the source addresses they can optionally modify their access control to examine any traffic destined towards their own customers originating from these source addresses. They can also tailor finer grained monitoring of such addresses. If the co-operating ASes are actively going to drop packets (i.e., filter) they have to install counters for the live duration of prefixes belonging to the fake announcements and ensure that they can modify ACL information to filter traffic based on destination addresses. This would require them to employ techniques similar to remote black-holing [11].

Co-operating with other ASes: costs and benefits Each of the ASes cooperating in the scheme can optionally augment the advertisements of dark prefixes with their own. As each co-operating AS filters out traffic at the earliest possible upstream location and passes on the information about source IP addresses, there is potential reduction of unwanted traffic entering the Internet through any of the cooperating network of ASes. Co-operating ASes can tailor their choice of dark prefixes, their length, and duration, based on the dark prefixes it sees from its neighbors. Although they cannot control the choices of other ASes, there is a potential for loose cooperation to maximize the ability to identify attackers. For example, attackers choice of address ranges and the thresholds chosen by individual ASes can be shared to help influence the selection of future dark prefixes and thresholds. When a group of ASes co-operate in the Mohonk scheme, the sum of the knowledge gained can greatly benefit all the cooperating entities. The positive network externalities of such co-operation results in benefits accruing to all the participants at low cost to the individual ASes. Note that such cooperation is obtained at relatively low cost without yielding any AS-specific information that may be viewed as sensitive. ASes that do not participate in the scheme and at the edge of the network of cooperating ASes will be viewed as a source of transmitters of unwanted traffic. Communication from such immediate nighbors may be downgraded if the threshold of such unwanted traffic exceeds a threshold. Since there is only potential benefits of learning about sources of such traffic, ASes have a logical reason to cooperate to watch for traffic towards various dark prefixes.

Finally, as a control measure, the originator of the Mohonk prefix announcements can test the effectiveness by including the community tag in some of the announcements and omitting it in some.

3. IMPLEMENTATION

There are four features of the BGP protocol that are of interest to Mohonk implementation. The first two are part of the BGP-4 standard while the other two are extensions that have been proposed. The first is the `Attribute` value field in a BGP announcement [12] (a BGP announcement consists of a prefix and optional attribute values). Of the 256 possible `Attribute` values, around half a dozen [13] are used frequently (AS_PATH, NEXT_HOP, LOCAL_PREF, MULTI_EXT_DISC, COMMUNITY, ORIGINATOR_ID, and CLUSTER_LIST). Mohonk uses the COMMUNITY field since it has no predefined meaning; i.e., it can be used for any experimental purpose without breaking any existing interpretation. Mohonk uses the COMMUNITY field to tag dark space advertisements as such. Community fields have been increasingly used as a way of signaling between adjacent and non-adjacent ASes. The second aspect is one of three specific reserved values [14] of the community field: 0xFFFFFF02 which informs a BGP neighbor not to pass on the community value further to its neighbors. This allows any Mohonk-compliant AS to restrict dark space advertisements to just their immediate neighbors. The third aspect is the Proxy Community Community value proposal [15] (implemented as a Flexible Community [16] value), which enables requesting an AS to send a community to a specific neighbor. The manner in which Mohonk will use this extension is tailoring it to a specific AS which is suspected to be the origin (or closest to the origin) of unwanted traffic. As the Proxy Community proposal points out, the originating AS can influence the selection of path and is a form of destination based traffic engineering. The last aspect is Cisco's policy accounting [17] mechanism whereby the BGP table-map command can be used to classify prefixes in the routing table by BGP attribute. Packet counters can be incremented on a per- input interface basis.

Setting parameters and generating announcement: An AS interested in participating in Mohonk would determine a set of dark prefixes of varying lengths it can use as dark prefixes. Based on its past traffic patterns it can select a threshold ranging from a few tens to a few hundreds of packets for categorizing traffic as a probing attack. The threshold and past traffic together enables coming up with the third parameter: advertisement duration of the dark prefix. Once these values are chosen, a routine BGP announcement is sent on one or more randomly chosen dark prefixes from the collection. The community attribute is set to `darkfake`. The reserved field of NO_ADVERTISE (0xffffff02) is set if the advertisement is meant only to the immediate peer and is not meant to be forwarded on. The optional value of targeting only a remote AS [15] is set if needed. The announcement is withdrawn after the determined duration (typically of the order of several hours).

As the simple schematic in Figure 1 shows, the probe traffic enters via AS 90210. The dark circles indicate the dark prefixes. AS 7 is shown sending regular Mohonk tagged advertisements to AS 4. AS 4 passes it on to ASes 314 and 1239, both of which participate in the scheme although they don't advertise their own dark prefixes. It is also shown (figuratively) bypassing AS 666 by using the Proxy Community attribute to have AS 10003 monitor traffic towards AS 7's dark prefix.

Recording incoming data and relaying it: On the associated honeypot machine, default replies are optionally sent back to the probing packets. The addresses are recorded and the packet count is checked to see if it has crossed the threshold associated with the prefix. Once the threshold has been crossed the address is sent to the co-operating set of ASes either piggybacked with the withdrawal or using out of band mechanism (such as [9]). The amount of information that is to be shared will guide is on the frequency and manner of sharing it between the interested ASes.

Measuring overhead due to Mohonk: Each new proposal to augment the work done in BGP communication is added overhead to the BGP speakers. While the potential reduction in unwanted traffic offsets the cost it is still useful to examine the overhead associated with Mohonk. The overhead consists of the following:

1. The one-time cost of identifying dark prefixes, threshold and announcement duration.

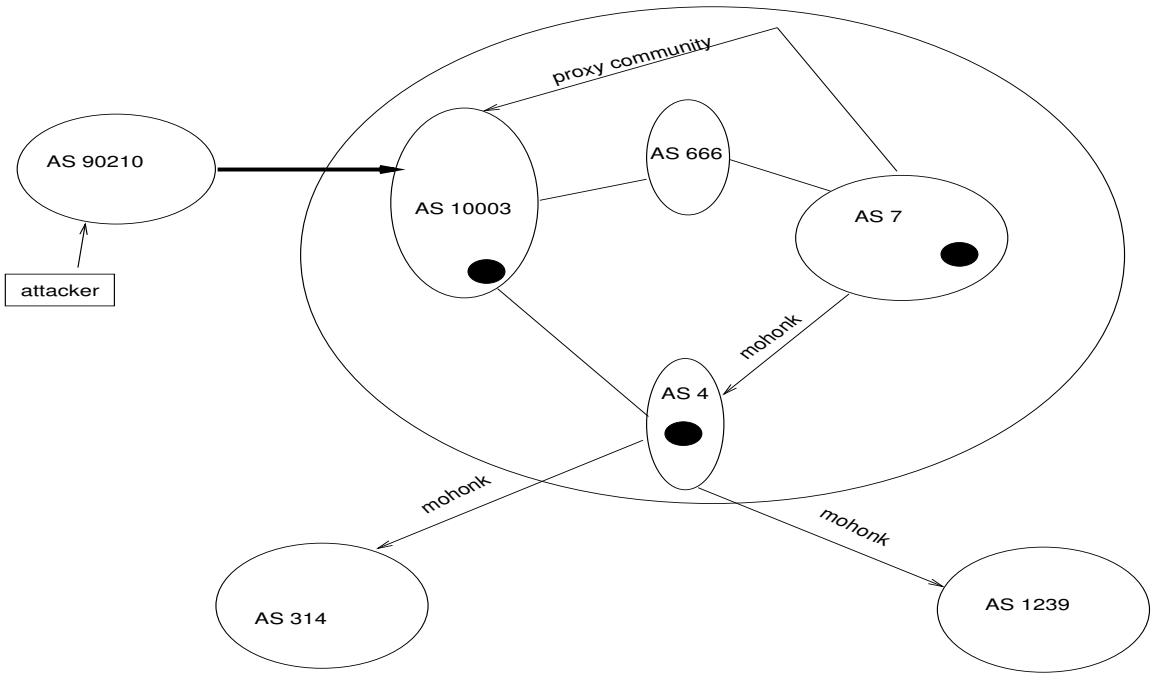

Figure 1: Mohonk Architecture

2. Processing Mohonk related advertisements and withdrawals.
3. The accounting of packet count for each fake announcements and recording the probe addresses.
4. Identifying the link associated with probe addresses if they belong to the AS.
5. Any policy-related overhead of using the probe addresses to change ACLs in routers or fine tuning anomaly detection on suspect links.

1 and 2 have very low cost. If there are too many Mohonk-related updates, it should not overwhelm any AS since ASes are free to ignore Community attributes. Given that no new connections have to be set up (advertisements and withdrawals are on existing BGP sessions) there is no significant network overhead. The cost related to 3 is likely to come down over time as the AS responsible for injecting the traffic can be targeted to be the one to do the accounting. Accounting only needs to be done by the AS at the edge of the co-operating set. The rest of the ASes do not have to keep track of counts associated with that prefix. The cost is thus distributed across the set of participating ASes and the edge AS on whose link the probe traffic entered will do the necessary accounting. 4 and 5 are opportunity costs and provide maximal benefits and so we discount them.

4. ATTACKS AGAINST MOBILE HONEYPOTS

A variety of attacks against honeypots occur routinely. The black hat community exchanges information to help each other identify honeypots to reduce their chances of being identified. The most common technique is the use of zombie machines or reflectors. Other avenues of attack against Mohonk are quite likely and we are scouring the various possibilities by consulting the detailed BGP attack catalog [18]. Meanwhile, we examine a few high-potential attacks that are possible.

Protection against reverse blacklisting: Information about attacking honeypots is available publicly [19]. A key difference in Mohonk is the setting up of honeypot machines to trace back attackers close to origination rather than to passively record information. The attackers cooperate by sharing information gleaned from their attacks not only of victims but also of traps, honeypots, and other anomaly detection systems. Commercial tools have been created to identify honeypots (e.g., Hon.eypot Hun.ter [20]) which tests a variety of hosts and port combinations to classify them as honeypot or not. Reverse blacklists have been created so that other attackers can avoid visiting sites that run honeypots. With Mohonk, the attackers have to locate the prefixes within the live duration of the announcement; thus they have to constantly monitor announcements. Even if they are able to glean the fake advertisements and avoid them in future scans, those prefixes can later be legitimately assigned to valid customers. Unlike domains set aside to detect email spam [21] and thus probers, the announcements are transient, random, and varied making it much harder for attackers to use the information. Additionally, it increases the cost for attackers by forcing them to do additional work that has limited value. Probing techniques that take into account the collection of dark prefixes over a period of time would still be faced with the risk of being discovered by *any* of the ASes participating in Mohonk. Each probing IP address that is discovered is shared with all the participating ASes.

Spoofed source addresses: A common concern is that even if the originator of scan traffic or other unwanted traffic is identified, the source addresses may have been spoofed. Re-

flector attacks are known to occur: With a spoofed source address SS1, SYN or ping packets are sent towards a victim V1 which then replies to SS1 (a RST/SYN-ACK or a ping response). The probability of using a dark address as SS1 is relatively low and thus falsely identifying V1 as a originator of such attacks is not very high. Further, since the duration of liveness of the advertised dark prefix is a parameter under the control of the advertiser and is often a short period of time, the potential for identifying significant number of victims is lower. Even if Mohonk is able to identify only spoofed source addresses, the information is of value. If a significant number of spoofed addresses are sending traffic through a certain link within an AS, the AS can monitor the link more closely. If a significant number of spoofed traffic originates from an AS, the information can be used as a way to possibly downgrade the links to that AS by its peers. One reason for the absence of wide deployment of traceback mechanisms is their cost. If it is possible to identify spoofed addresses significantly closer to their origination, this might spur the AS in question to take action. An alternative way [22] to track down spoofed addresses can be done via Cisco Express Forwarding [23].

Black-hat ASes: What if one of the ASes that is not cooperating is a black-hat AS? They are known to exist and information from them may be viewed as suspect. They may not be willing to cooperate in which case its peers are free to downgrade the links to them. If they actively co-operate and feed false source addresses knowing the destination dark prefixes, then they would still be viewed as a problematic AS. Feeding false source addresses including ones that belong to one of the cooperating set of ASes would help unmask them. The downside is thus higher for black-hat ASes. Alternately, black-hat ASes can send information about current list of dark prefixes to probing entities. This requires them to be in constant touch with all their 'friends' and constantly update a diverse set of changing prefixes.

Fake fake announcements: What about the (existing) problem of fake announcements? Nothing prevents a black-hat AS from advertising (especially withdrawing) some other ASes prefixes. Many ISPs successfully filter any information coming from their customers and the Tier-1 ISP's route filter announcements on their peering sessions. We don't believe that Mohonk makes the problem any worse. If, however, a fake announcement is sent marking certain prefixes as dark, diligent ISPs will be able to detect the black-hat AS.

5. RELATED WORK

To the best of our knowledge this is the first proposal to make honyepots mobile and for the purpose of tracing unwanted traffic closer to its originating point. The closest related work is that of Turk [24], where an operational technique is discussed to remotely trigger blackholing via BGP communities (the original proposal on this is from 1999 [11]). The Secure origin BGP (soBGP) Certificates [25] proposal allows routers to verify the origins of the announcements using out of band mechanisms. Deployment of this proposal would ensure that black-hat ASes cannot advertise unauthorized prefixes; however this proposal has not yet been deployed anywhere.

There is considerable prior work in single site honeypots, multi-site honeypots, and tracing back traffic. *Honeyfarms* [26], used to detect worms automatically, are a centralized collection of honeypots (and related analysis tools) that receives suspicious traffic redirected to it from different detection devices spread around the Internet. *Wormholes* are simple appliances used to securely transmit the suspicious traffic to the honeyfarm. A set of k honeypots will be able detect a worm when roughly 1/k of the vulnerable machines are infected. Honeyfarm uses virtual machine images to implement honeypots creating both a "vulnerability signature" and a possible attack signature. The detection is based on infected honeypots and not traffic from the wormhole. The telescope work [3] presents global views on DoS attacks using local monitoring.

Genii [27], the so-called second generation of honeypots, reduced effort to deploy honeypots and are generally harder to detect. Genii relies on a separate, secure network that is used for administration purposes making the gateway difficult to detect due to the absence of associated MAC addresses, or even routing hops or TTL decrements. However, as the authors themselves admit, in the arms race against attackers, security through obscurity has never had a long shelf life of success.

6. PRESENT AND FUTURE WORK

We are in the process of deploying honeypots using the dark space available to us in AT&T. We are running *honeyd* on a few machines to gather data to identify the right prefix lengths and durations of the fake announcements. We are also planning to communicate with several friendly ASes to see if they would be willing to cooperate with us on Mohonk.

7. ACKNOWLEDGMENTS

The Mohonk work has benefited from conversations with several people: Steve Bellovin for general thoughts on tracing traffic back, Jay Borkenhagen and Rich Krapniewski for thoughtful suggestions on operational matters, Jennifer Rexford for pointing out useful BGP-related material, and Yin Zhang for worrying aloud about a few possible attacks. Tim Battles provided valuable feedback on operational issues and is helping in gathering data. The work has also benefited by discussions with Randy Bush and Tim Griffin. I thank Zihui Ge, Zhuoqing Morley Mao, Jennifer Rexford, and Jia Wang for their thoughtful comments on the paper.

8. REFERENCES

[1] Lance Spitzner, "Honeypots: Definitions and Value of Honeypots." `http://www.tracking-hackers.com/papers/honeypots.html`.

[2] Shaheem Motlekar, "Honeypots: Frequently Asked Questions." `http://www.tracking-hackers.com/misc/faq.html`.

[3] David Moore, "Network Telescopes: Observing Small or Distant Security Events," August 2002. Usenix Security Symposium, `www.caida.org/outreach/presentations/2002/usenix_sec/usenix_sec_2002_files/v3_document.html`.

[4] "Hackbusters - Homepage." `http://hackbusters.net`.

[5] Vinod Yegneswaran and Paul Barford and Somesh Jha, "Global Intrusion Detection in the DOMINO Overlay System," in *Proceedings of ISOC 2004*, February 2004. `http://www.cs.uwisc.edu/~barford/isoc04.ps`.

[6] N. Provos, "Honeyd - A virtual honeypot daemon," in *Proceeding of the 10th DFN-CERT Workshop*, February 2003. http://www.cert.dfn.de/events/ws/2003/dfncert-ws2003-f1.zip.

[7] "KFSensor." http://www.keyfocus.net/kfsensor/.

[8] "Subscription via Multihop eBGP4." http://mail-abuse.org/rbl/usage.html#BGP.

[9] Geoffrey Goodell et al., "Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing," in *10th Annual Network and Distributed System Security Symposium*, February 2003. www.eecs.umich.edu/~pdmcdan/docs/ndss03.pdf.

[10] Zesheng Chen and Lixin Gao and Kevin Kwiat, "Moeling the spread of Active Worms," in *Proceedings of Infocom*, March 2003. http://www.cs.umass.edu/~gao/paper/AAWP.pdf.

[11] A. Bligh, "Using a Well Known Community to mitigate the effects of a Denial of Service Attack," July 1999. http://www.merit.edu/mail.archives/nanog/1999-07/msg00083.html.

[12] Y. Rekhter and T. Li, "Border Gateway Protocol 4 (BGP-4)," RFC 1771, IETF, March 1995. http://www.rfc-editor.org/rfc/rfc1771.txt.

[13] Timothy G. Griffin, "An Introduction to Interdomain Routing and the Border Gateway Protocol (BGP)," November 2002. http://www.cambridge.intel-research.net/~tgriffin/talks_tutorials/tutorials/icnp2002/.

[14] R. Chandra and P. Traina and T. Li, "BGP Communities Attribute," RFC 1997, IETF, August 1996. http://www.rfc-editor.org/rfc/rfc1997.txt.

[15] S. Agarwal and T. G. Griffin, "BGP Proxy Community Community," January 2004. http://www.ietf.org/internet-drafts/draft-agarwal-bgp-proxy-community-00.txt.

[16] A. Lange, "Flexible BGP Communities," March 2004. http://www.ietf.org/internet-drafts/draft-lange-flexible-bgp-communities-02.txt.

[17] "BGP Policy Accounting." http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00800ad90a.html.

[18] S. Convery and D. Cook and M. Franz, "An Attack Tree for the Border Gateway Protocol," September 2003. http://www.ietf.org/internet-drafts/draft-convery-bgpattack-01.txt.

[19] Joseph Corey, "Local Honeypot Identification." http://www.phrack.org/fakes/p62/p62-0x07.txt.

[20] "Send-Safe Honeypot Hunter." http://www.send-safe.com/honeypot-hunter.php.

[21] Jens Knoell, "Honeypots: Using specialized honeypots to build up-to-date spam blacklists?," September 2003. http://seclists.org/lists/honeypots/2003/Jul-Sep/0254.html.

[22] R. Thomas, "Tracking Spoofed IP Addresses Version 2.0." www.cymru.com/Documents/tracking-spoofed.html.

[23] "Cisco Express Forwarding (CEF)." http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/cef_wp.htm.

[24] D. Turk, "Configuring BGP to Block Denial-of-Service Attacks," March 2004. http://www.ietf.org/internet-drafts/draft-turk-bgp-dos-06.txt.

[25] B. Weis, "Secure Origin BGP (soBGP) Certificates," October 2003. http://www.ietf.org/internet-drafts/draft-weis-sobgp-certificates-01.txt.

[26] Nick Weaver, "Wormholes and honeyfarm," in *WIP session: Usenix Security Symposium*, 2003. http://www.ieee-security.org/Cipher/ConfReports/2003/CR2003-USENIX.html.

[27] "Know Your Enemy: GenII Honeynets." www.linuxvoodoo.net/resources/security/gen2/.