ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

IP Tracebaking on an Hybrid Approach

AR.Arunachalam
Assistant Professor , Department of CSE , Bharath University, Chennai, India

ABSTRACT: Emergence and wide spread of internet has enlarged the space to security threat. Attackers hide themselves through IP spoofing and launch attacks that makes an ordinary man a culprit.To find out the actual source, researchers work on various trace backing schemes. In this paper we propose a new hybrid trace backing scheme with packet counters.Our scheme has remarkable advantages (1) simple and efficient (2)significantly resistant to attacks (3)Storage requirement to every router is bounded above the number of paths to the router (4)achieves zero false positive and zero false negatice rates in path reconstruction.

I.INTRODUCTION

One of the most serious threats to the Internet security is a DoS (Denial ofService) attack, where an attacker attempts to make a target host (called avictim) fail by sending a huge number of packets to the host . Inrecent years, a DDoS (Distributed DoS) attack, where there are many attackersscattered over the Internet, has become more prevailing .We call a path along whichan attack packet traverses from one attacker to the victim an attack path.A countermeasure against DoS/DDoS attacks is called IP tracebackIn IP traceback schemes, each router on attack paths stores informationabout the paths on itself or on packets. Then the victim uses the information
to find out the attackers.IP traceback schemes are roughly classified two-fold:deterministic packet marking(DPM),as probabilistic packetmarking (PPM for short) protocols and logging ones. In PPM protocols, each router probabilistically writes path information onto the packets it receives. On the other hand, logging IP trace back protocols make each participating router sample packets and store path information on itself. PPM and logging protocols have some advantages.
In this paper we shall propose a new hybrid IP trace back scheme. A novel idea of our scheme is the introduction of a counter on each packet header. (1) it is simple and efficient, (2) it is highly resistant to attacks, (3) it needs a lower sampling rate compared with previous work, e.g., only 1% is enough,(4) its false positive/negative rates are lower. This paper is organized as follows. We discuss related work in Sect. 2 and shall propose a novel IP trace back in Sect. 3. Then we thoroughly evaluate our scheme in Sect. 4 and Sect. 5. Finally we give conclusion in Sect. 6.

II.RELATED WORK

Packet marking can be put into two categories. Deterministic Packet Marking(DPM) and Probablistic Packet Marking(PPM). PPM does not needstorage resource of routers, although, it generally requires the victim to receive alarge number of packets before he can reconstruct the attack tree. On the otherhand, in logging schemes, the number of packets for attack tree recovery can besmall. However, logging schemes impose heavy load and require extremely large storage space on the routers[1][2]. Now, for a recent example of IP traceback protocols, let us consider the work in RIHT: A novel hybrid IP traceback scheme a p.mark value is calculated to find out the flow of packet and to find the attack. This approach considers a large amount of calculation which is time consuming.
In summary, we develop a highly efficient IP traceback scheme by considering correlation of packet sampling all over a whole attack path[3][4].

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

III.EXISTING SYSTEM

Current traceback schemes tends to log packets of information on routers. Most current tracing schemes that are designed for software exploits can be categorized into three groups. single packet, packet logging and hybrid IP traceback. The fundamental idea of packet logging is to log a packet's information on routers. The method used in the existing system is RIHT.

Existing system contains a hybrid IP traceback scheme with packet logging aiming to have a fixed storage requirement for each router. Like MRT and MORE, RIHT marks interface numbers of routers on packet so as to trace the path of packets. Since the marking field on each packet is limited, hence all information about the packets journey from source to destination cannot be stored. The main disadvantage of the existing system is that it suffers from fragmentation problem and it is a time consuming process[5].

IV.PROPOSED SYSTEM

The proposed system, we provide a new hybrid ip traceback scheme which uses packet counter for packet marking and path reconstruction

The entire work of this system is divided into five modules

1. Network topology construction
2. Path selection
3. Packet sending
4. Packet marking and logging
5. Path reconstruction

V.NETWORK TOPOLOGY CONSTRUCTION

A network topology may consist many number of routers that are connected with LANs. Thus, a router can either receive data from the nearer router or from the LAN. A border router receives packets from its LAN. A main router receives packets from other routers. The number of routers connected to a single router is called the degree of the router[6]. This is calculated and stored in a table, the upstream interfaces of each router also have to be found and stored in the interface table.

Path Selection:

The path is said to be the way in which the selected packet or file has t5o be sent from the source to destination.the upstream interfaces of each routers have to be found and it is stored in the interface table.With the help of the interface table the selected source and destination can be defined[7].

Packet sending:

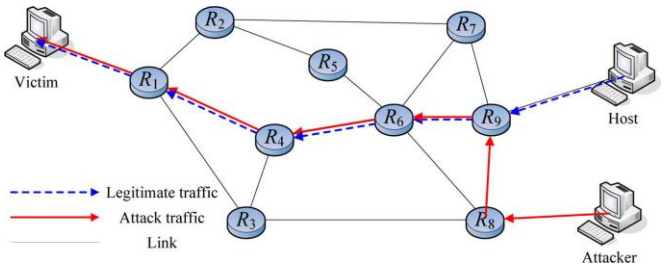
In the packet or file transformation process, the packet is sent along the defined path fom the source LAN to the destination LAN. The destination LAN receives the packet and verifies whether it has been sent along the defined path or not.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015



Packet marking and logging:

We design a five bit space on each packet header as a counter which is denoted as p.counter In our scheme, if a router on an attack path decides to sample a packet P with some probability , then it increments p.counter by one, stores some information on itself, and finally passes the packet to an adjacent router. Consequently, the greater the value of P.counter is, the larger the number of routers on the attack path that store information of P is. In other words, a packet with a large counter value is useful when we recover the attack tree[8]. Therefore, when we sample a packet, if we probabilistically prefer a packet with a larger counter value to one with a smaller value, then we can improve the correlation factor of packet sampling and have more useful packets for traceback later

Bit offset	0-3	4-7	8-15	16-18	19-31
0	Version	Header length	TOS	Total length	
32	Identification field			Flag	Fragment offset
64	TTL		Protocol	Header checksum	
96	Source address				
128	Destination address				
160	Options				
160 or 196+	Payload (first 8bytes)				

Path reconstruction:

Once the packet has reached the destination after applying the algorithm three it checks whether it has sent from the correct upstream interfaces. If any of the attack is found, it request for path reconstruction. Path reconstruction is the process of finding the new path for the same source and the destination for which no attack can be made.

Algorithms :

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

```
begin
1.  UI_i = mark_req % (D(R_i) + 1) – 1
2.  if UI_i = -1 then
3.      index = mark_reg / (D(R_i) + 1)
4.      if not index = 0 then
5.          UI_i = HT[index].UI
6.          mark_old = HT[index].mark
7.          send reconstruction request with mark_old to upstream router by UI_i
8.      else
9.          this router is the nearest border router to the attacker
10.     endif
11. else
12.     mark_old = mark_req / (D(R_i) + 1)
13.     send reconstruction request with mark_old to upstream router by UI_i
14. endif
end
```

Algorithm for path reconstruction

Sampling procedure at router R:
for each packet P
x is chosen uniformly at random between 0 and 1
p ← compute prob(P.counter)
if (x < p) **then** _ i.e, with probability p
P.counter ← P.counter +1
Store digest of P

VI.SECURITY CONSIDERATION

In this section we briefly discuss security of our scheme. First note that all attackers are supposed to be located at the leaves of an attack tree. Therefore, an attacker could affect security of our scheme only by forging packet counters[9].

More specifically, all that the attacker can do is only to set to some value the counter of a packet that he injects into the network. However, such a forge by the attacker cannot be a threat to our scheme for the following reason. Namely, a large value of a packet counter given by the attacker only leads to an increase of the sampling probability of the packet, which in turn ends with increasing the correlation of packet sampling and then finally with a more efficient traceback process. Therefore, such an "attack" can never be an attack in a true sense, but rather it leads the victim to a situation that is more beneficial to him[10].
Thus, a possible attack that attackers at the leaves can make would be to always set the lowest values to packet counters, that is, to always initialize the counters to zero.[11] This is indeed the worst case scenario to our protocol because in such a case correlation of packet sampling would be forced to be as low as possible and then traceback processes later would be made more difficult.
Fortunately, again, such an attack above cannot be effective.In summary, we can conclude that our scheme is highly resistant to attacks.[12]

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

False Positive and False Negative Rates

When a router is mistaken for an attack router, we call it "false positive". When we fail to trace back to an attacker, we call it "false negative". Even if the logged data is not cleared,existing systems still are unable to avoid the false positive problem. In MRT, a router logs the marking fields of packets, which are indexed by the digests of the packets, on the log table. In MORE, a router uses different log tables, which are associated with , to log the marking fields of packets indexed by the digests of the packets[11]. Therefore, the false positive rates of MRT and MORE are greater than 0 even without refreshing if a collision of digests happens in a log table.[13] On the other hand, in RIHT, since we mark index on each logged packet's marking field, under the guidance of each index, we can just obtain the logged data from the hash table and circumvent the collision problem. Therefore, without any chance of a collision in our scheme, our false positive rate is 0, hence higher accuracy.[14]

Packet Identity

In the same route, every packet's marking field is the same on an arbitrary router. So, a packet's marking field is often seen as a packet identifyand used to help us identify an attack packet's source and then filter malicious packets[15]. But in the existing schemes, we are unable to identify a packet's.[16] For this reason, the victims are confused and unable to identify the packet's source simply from the comparison of marking fields. In our scheme, the marking fields of packets are identical to each other on a router if and only if they travel on the same route to the router. Therefore, when filtering malicious packets, marking field of our scheme's can act as a packet identity and avoid certain confusion.[17]

VII.CONCLUSION

In this paper, we propose a new hybrid IP traceback schemefor efficient packet logging aiming to have a fixed storage requirement (under 320 K bytes, based on the CAIDA's skitter data set) in packet logging without the need to refresh the logged tracking information. Also, the proposed scheme has false negative and zero false positive rates in an attack-path reconstruction. Apart from these properties, our scheme can also deploy a marking field as a packet identity to filter malicious traffic and secure against DoS/DDoS attacks. Consequently, with high accuracy, a low storage requirement, and fast computation.

REFERENCES

1. H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in *Proc. of the 14th USENIX Systems Administration Conferrence*, December 2000.
2. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "High data rate for coherent optical wired communication using DSP", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) 4772-4776.
3. G. Sager, "Security fun with OCxmon and cflowd," in *Internet 2 working group meeting*, November 1998.
4. Selva Kumar S., Ram Krishna Rao M., Deepak Kumar R., Panwar S., Prasad C.S., "Biocontrol by plant growth promoting rhizobacteria against black scurf and stem canker disease of potato caused by Rhizoctonia solani", Archives of Phytopathology and Plant Protection, ISSN : 0323-5408, 46(4) (2013) pp.487-502.
5. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," *IEEE/ACM Transactions on Networking*, vol. 9, June 2001.
6. B.Vamsi Krishna, A New Technique for Elimination of Harmonics Using Three Phase Shunt Active Filter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 5596-5602, Vol. 2, Issue 11, November 2013
7. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Optical ring architecture performance evaluation using ordinary receiver", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4742-4747.
8. A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, S. Kent, and W. Strayer, "Single-packet IP traceback,"*IEEE/ACM Transactions on Networking*, vol. 10, December 2002.
9. A.Geetha, Universal Asynchronous Receiver / Transmitter (UART) Design for Hand Held Mobile Devices, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2231-5381, pp 25-26, Volume 3 Issue 1 No1 – January 2012.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

10. Subha Palaneeswari M., Abraham Sam Rajan P.M., Silambanan S., Jothimalar, "Blood lead in end-stage renal disease (ESRD) patients who were on maintainence haemodialysis", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(10) (2012) pp.1633-1635.
11. B. Bloom, "Space/time trade-offs in hash coding with allowable errors,"*Communications of ACM*, vol. 13, July 1970.
12. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Performance analysis of resilient ftth architecture with protection mechanism", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4737-4741
13. D. Song and A. Perrig, "Advanced and authenticated marking schemesfor IP traceback," in *Proc. of IEEE INFOCOM*, April 2001.
14. U. Tupakula and V. Varadharajan,"A practical method tocounteractdenial of service attacks," in *Proc. of the26thAustralasianComputer Science Conference*, February 2003.
15. A.Geetha, Face Recognition Using OPENCL, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , ISSN (Print) : 2320 – 3765, pp- 7148-7151, Vol. 3, Issue 2, Febuary 2014.
16. B.Mehala, Mrs.Anitha Sampath Kumar, Design and Implementation of Resonant Circuit Based On Half-Bridge Boost Rectifier with Output Voltage Balance Control, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 9370-9378, Vol. 3, Issue 5, May 2014
17. B.Vamsi Krishna, Starting Inrush Current Control of Three-Phase Induction Motors for Dispersed Generating Systems, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 6411-6422, Vol. 2, Issue 12, December 2013