The New Cell-Counting-Based Against Anonymous Proxy

Yadarthugalla Raju
M.Tech Student, Department of CSE,
Dr.K.V.S.R.I.T, Kurnool.

K. Pavan Kumar
Assistant Professor, Department of IT,
Dr.K.V.S.R.I.T, Kurnool.

Abstract

Various low-latency state of an individual's personal identity, or personally identifiable information, being publicly unknown, such as anonymity network and proxy server have been designed to provide anonymity service for users. In order to hide the communication of users, most of the anonymity systems pack the application data into equal-sized cells. By the extensive experiments on anonymity network, we found that the size of IP packets in the internet communication method intended to enable online anonymity network can be very dynamic because a cell is an application concept and the IP layer may repack cells. Based on this finding, we investigate a new cell-counting-based attack against Tor, which allows the attacker to confirm anonymous communication relationship among users very quickly. In this attack, by marginally varying the number of cells in the target traffic at the malicious exit onion router, the attacker can embed a secret signal into the variation of cell counter of the target traffic. The embedded signal will be carried along with the target traffic and arrive at the malicious entry onion router. Then, the onion router will detect the embedded signal based on the received cells and confirm the communication relationship among users. We have implemented this attack against anonymity network, and our experimental data validate its feasibility and effectiveness. There are several unique features of this attack. First, this attack is highly efficient and can confirm very short communication sessions with only tens of cells. Second, this attack is effective, and its detection rate approaches 100% with a very low false positive rate. Third, it is possible to implement the attack in a way that appears to be very difficult for the honest participants to be detect.

Keywords--- *anonymity network, cell counting, onion router, signal, mix networks.*

1.Introduction

Concerns about privacy and security have received greater attention with the rapid growth and public acceptance of the Internet, which has been used to create our global E-economy. Anonymity has become a necessary and legitimate aim in many applications, including anonymous Web browsing, location-based services (LBSs), and Evoting. In these applications, encryption alone cannot maintain the anonymity required by participants. In the past, researchers have developed numerous anonymous communicate on systems. Generally speaking, mix techniques can be used for either message-based (high-latency) or flow-based (low-latency) anonymity applications. E-mail is a typical message-based anonymity application, which has been thoroughly investigated. Research on flow-based anonymity applications has recently received great attention in order to preserve anonymity in low-latency applications, including Web browsing and peer-to-peer file sharing. To degrade the anonymity service provided by anonymous communication systems, traffic analysis attacks have been studied. Existing traffic analysis attacks can be categorized into two groups: passive traffic analysis and active water marking techniques. Passive traffic analysis technique will record the traffic passively and identify the similarity between the sender's outbound traffic and the receiver's inbound traffic based on statistical measures. Because this type of attack relies on correlating the timings of messages moving through the anonymous system and does not change the traffic characteristics, it is also a passive *timing* attack.

2.Implementation

Passive traffic analysis technique will record the traffic passively and identify the correlation between sender's outbound traffic and receiver's inbound traffic based on statistical measures. This type of technique requires a relatively long period of traffic observation for a reasonable detection rate. The idea is to actively introduce special signals into the sender's outbound traffic with the intention of recognizing the embedded signal at the receiver's inbound traffic. Encryption does not work, since packet headers still reveal a great deal about users. In this project, we focus on the active watermarking technique, which has been active in the past few years. proposed a flow-marking scheme based on the direct sequence spread spectrum technique by utilizing a pseudo-noise code. By interfering with the rate of a suspect sender's traffic and marginally changing the traffic rate, the attacker can embed a secret spread-spectrum signal into the target traffic. The embedded signal is carried along with the target traffic from the sender to the receiver, so the investigator can recognize the corresponding communication relationship, tracing the messages despite the use of anonymous networks. However, in order to accurately confirm the anonymous communication relationship of users, the flow-marking scheme needs to embed a signal modulated by a relatively long length of PN code, and also the signal is embedded into the traffic flow rate variation. Houmansadr. proposed a nonblind network flow watermarking scheme called RAINBOW for stepping stone detection.

3.Design Goals

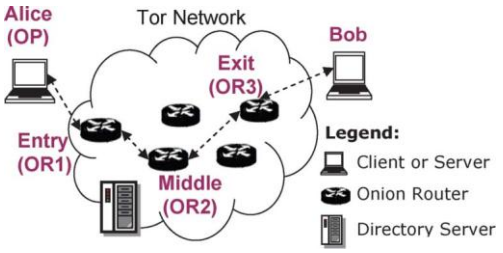

Fig: Tor network

We first overview the components of Tor. We then present the procedures of how to create circuits and transmit data in Tor and process cells at onion routers.

COMPONENTS OF TOR

Tor is a popular overlay network for providing anonymous communicate on over the Internet. It is an open-source project and provides anonymity service for TCP applications . As shown in Fig. 1, there are four basic components in Tor.

1) *Alice* (i.e., *Client*)
   The client runs a local software called *onion proxy* (*OP*) to anonymize the client data into Tor.
2) *Bob* (i.e., *Server*)
   It runs TCP applications such as a Web service.
3) *Onion routers (ORs)*
   Onion routers are special proxies that relay the application data between Alice and Bob. In Tor, transport-layer security (TLS) connections are used for the overlay link encryption between two onion routers. The application data is packed into equal-sized cells.carried through TLS connections.

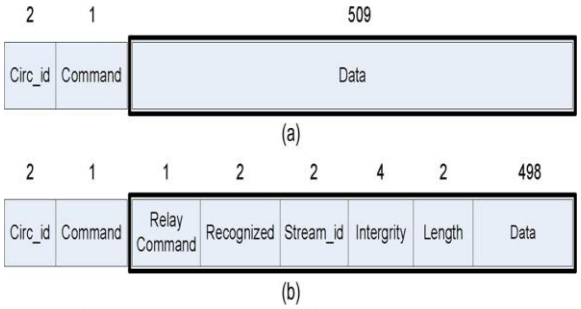

Fig.Cell format by Tor. (a) Tor cell format. (b) Tor relay cell format.

4) *Directory servers*
   They hold onion router information such as public keys for onion routers. Directory authorities hold authoritative information on onion routers, and directory caches download directory information of onion routers from authorities. A list of directory authorities is hard-coded into the Tor source code for a client to download the information of onion routers and build circuits through the Tor network.

DATA TRANSMISSION

In Tor, an maintains a connection to other on demand. The uses a way of source routing and chooses several from the locally cached directory, downloaded from the directory caches. The number of the selected is referred as the path length. We use the default path length of three as an example. The iteratively establishes circuits across the Tor network and negotiates a symmetric key with each, one hop at a time, as well as handles the streams from client applications. The side of the circuit connects to the requested destinations and relays the data. We now illustrate the procedure that the establishes a circuit and downloads a file from the server.

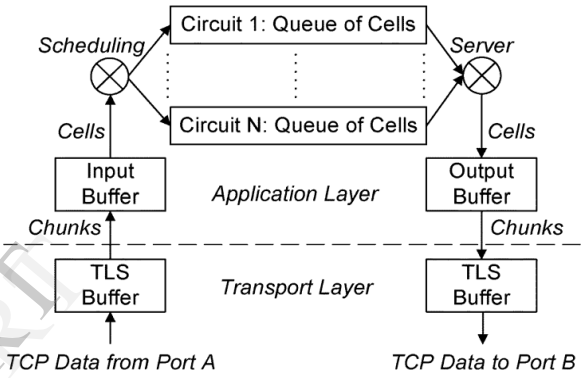

Fig. Processing the cells at onion routers

CELLS AT ONION ROUTERS

To begin with, the onion router receives the data from the connection on the given port *A*. After the data is processed by protocols, the data will be delivered into the buffer of the connection. When there is pending data in the buffer, the read event of this connection will be called to read and process the data. The connection read event will pull the data from the buffer into the connection input buffer. Each connection input buffer is implemented as a linked list with small chunks. The data is fetched from the head of the list and added to the tail. After the data in the TLS buffer is pulled into the connection input buffer, the connection read event will process the cells from the connection input buffer one by one.

4.Cell-Counting-Based Attack

In this section, we first show that the size of IP packets in the Tor network is very dynamic. Based on this finding, we then introduce the basic idea of the cell-counting-based attack and list some challenging issues related to the attack and present solutions to resolve those issues.

DYNAMIC IP PACKT SIZE OF TRAFFIC OVER TOR

In Tor, the application data will be packed into equal-sized cells. Nonetheless, via extensive experiments over the Tor network, we found that the size of IP packets transmitted over Tor is dynamic. It can be observed that the size of packets from the sender to the receiver is random over time, and a large number of packets have varied sizes, other than the cell size or maximum transmission unit (MTU) size.

These observations can be reasoned as follows.

1) The varied performance of onion routers may cause cells not to be promptly processed. According to cell processing in. if an onion router is overloaded, unprocessed cells will be queued. Therefore, cells will be merged at the IP layer and sent out together. Those merged cells may be split into multiple MTU-sized packets and one non-MTU-sized packet.
2) Tor network dynamics may incur those non-MTU-sized IP packets as well. If the network between onion routers is congested, cells will not be delivered on time. When this happens, cells will merge, and non- MTU-sized IP packets will show up.

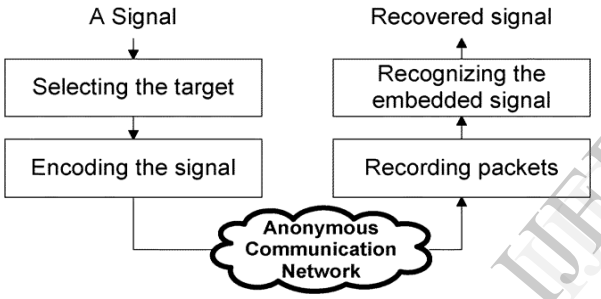

FIG:Cell-counting-based attack

BASIC IDEA OF CELL-COUNTING-BASED ATTACK

As we stated above, the packet size observed at the client shows a high probability to be random because of the performance of onion routers and Internet traffic dynamics. Motivated by this finding, we investigate a new cell-counting-based attack against Tor, which allows the attacker to confirm anonymous communication relationship among users very quickly.

5. Related Works

A good review of mix systems has been much research on degrading anonymous communication through mix networks. Existing traffic analysis attacks against anonymous communication can largely be categorized into two groups: passive traffic analysis and active watermarking techniques. Passive traffic analysis techniques have shown that the attacks record the traffic passively and identify the similarity between server's outbound traffic and client's inbound traffic. Other recent research works have shown that the attackers can infer sensitive information from the encrypted network traffic by examining patterns in terms of the sizes of packet and its timing.

5.Conclusion

In this paper, we introduced a novel cell-counting-based attack against Tor. This attack is difficult to detect and is able to quickly and accurately confirm the anonymous communication relationship among users on Tor. An attacker at the malicious exit onion router slightly manipulates the transmission of cells from a target TCP stream and embeds a secret signal (a series of binary bits) into the cell counter variation of the TCP stream. An accomplice of the attacker at the entry onion router recognizes the embedded signal using our developed recovery algorithms and links the communication relationship among users. Our theoretical analysis shows that the detection rate is a monotonously increasing function with respect to the delay interval and is a
monotonously decreasing function of the variance of one way
transmission delay along a circuit. Via extensive real-world experiments on Tor, the effectiveness and feasibility of the attack is validated. Our data showed that this attack could drastically and quickly degrade the anonymity service that Tor provides. Due to Tor's fundamental design, defending against this attack remains a very challenging task that we will investigate in our future research.

6.References

[1] Q. X. Sun, D. R. Simon, Y. Wang, W. Russell, V. N. Padmanabhan, and L. L. Qiu, "Statistical identification of encrypted Web browsing traffic," in *Proc. IEEE S&P*, May 2002, pp. 19–30.

[2] X.Fu,Y.Zhu,B.Graham,R.Bettati,andW.Zhao,"On flow marking attacks in wireless anonymous communication networks," in *Proc.IEEE ICDCS*, Apr. 2005, pp. 493–503.

[3] L. Øverlier and P. Syverson, "Locating hidden servers," in *Proc. IEEE S&P*, May 2006, pp. 100–114.

[4] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: Proposal of a type III anonymous remailer protocol," in *Proc. IEEE S&P*,May 2003, pp. 2–15.

[5] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *Proc. 13th USENIX Security Symp.*, Aug. 2004, p. 21.

[6] "Anonymizer, Inc.," 2009 [Online]. Available: http://www.anonymizer.com/

[7] A. Serjantov and P. Sewell, "Passive attack analysis for connection based anonymity systems," in *Proc. ESORICS*, Oct. 2003, pp. 116–131.

[8] B.N.Levine,M.K.Reiter,C.Wang,andM.Wright, "Timing attack sin low-latency MIX systems," in *Proc. FC*, Feb. 2004, pp. 251–565.

[9] Y.Zhu,X.Fu,B.Graham,R.Bettati,andW.Zhao,"On flow correlation attacks and countermeasures in Mix networks," in *Proc. PET*, May 2004, pp. 735–742.

[10] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," in *Proc. IEEE S&P*, May 2006, pp. 183–195.

[11] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, "Low resource routing attacks against anonymous systems," in *Proc. ACM WPES*, Oct. 2007, pp. 11–20.

[12] W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao, "DSSS-based flow marking technique for invisible traceback," in *Proc. IEEE S&P*,May2007, pp. 18–32.

About the Authors

Yadarthugalla Raju, recieved his B.TECH. degree from Jawaharlal Nehru University, Anantapur, India in the year 2010. He is currently pursuing M.Tech in Computer Science and Engineering from Dr. K.V.S.R.I.T, Kurnool, India. His research interests include networkings.

K.Pavan Kumar, received his B.Tech degree in Computer Science and Engineering from JNTU, Hyderabad, India in the year 2006 and M.Tech in Computer Science from JNTU Hyderabad, India, in the year 2009. He is currently working as a Assistant Professor at Dr.K.V.S.R.I.T, Kurnool, India. His research interests include Mobile Ad-hoc Networks, Computer Networks and Cloud Computing.