GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ANONYMITY BASED ATTACK ON TOR

Miss.Pallavi Bhujbal *[1] & Prof. Pankaj R.Chandre[2]
Research Scholar,Department of computer Engineering,Spcoe college of Engineering, Pune(MH),India*[1]
Assistant Professor,Department of computer Engineering,Spcoe college of Engineering, Pune(MH),India[2]
palbhujbal05@gmail.com*[1]

ABSTRACT

In the today's world there is mainly people are concentrate on the security and privacy of the data. As there is some change in security system behavior it not as per user intention. In the network some people make unintentional expose of personal information, or relationships and other things in front of people. Technology gives us solution for these types of exposures that is encryption and decryption for data i.e. change view and appearance of data for other or unknown persons. In networking there are mainly two types of attacks Passive and Active attack. Passive i.e. only monitoring the system network and data which is send. But the active attack is focus about the only change in data send by client. Attackers interested in the changing of data and to get detail about the communication happen in the sender and receiver. In TOR, attack happen at the exit onion router. While searching basically this attack is based on active attacks. But main problem in this type is degrading attacks and hidden services. In this attack attacker select particular IP packet at exit onion router and changes that packet. So our aim is to detect attacker and degrade anonymous services.

Keywords- Mix network, Onion routing network, Hidden services.

I. INTRODUCTION

A network is simply defined as something that connects things together for a specific purpose. The term network is used in a variety of contexts, including telephone, television, computer, or even people networks. A computer network connects two or more devices together to share a nearly limitless range of information and services, including: Documents, Email and messaging, Websites, Databases, Music, Printers and faxes, Telephony and video-conferencing On the most fundamental level, a computer network is an interconnected collection of devices that enables you to store, retrieve, and share information. Commonly connected devices include personal computers (PCs), minicomputers, mainframe computers, terminals, workstations, thin clients, printers, fax machines, pagers, and various data storage devices. Recently, other types of devices have become network connect-able, including interactive televisions, videophones, hand-held devices and navigational and environmental control systems. Eventually, networked devices everywhere will providetwo-way access to a vast array of resources on a global computer network through the largest network of all, the Internet. In today's business world a computer network is more than a collection of interconnected devices. For many businesses the computer network is the resource that enables them to gather, analyze, organize, and disseminate information that is essential to the probability.

A) Network Security

Network security has become more important to personal computer users, organizations and the military. With the advent of the internet security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allowsfor the appropriate security to emerge. Many businesses secure themselves from the internet by mean so firewallsand encryption mechanisms. The businesses create an "Intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

B) Locating Hidden Services in TOR

Hidden servers offering some kind of service to the user of the TOR network. For example, web pages, mail accounts, login services, etc. One of the measure vulnerability for a hidden service in TOR is the servers selection of the first and last node in the communication path.. This is because the low latency requirements make it easy to confirm the timing signature of traffic flowing (in both direction) over circuit[2].

II. LITERATURE SURVEY

A)Basic Concept

The basic idea of onion routing can be traced back anonymous email. It introduces a network consisting of a large number of "MIX" nodes. MIX nodes serve the simple role of accepting emails encrypted with their public keys, decrypting them, and then sending them on. Each node would also perform certain timing alteration of the emails to make it harder for a network observer to trace the path that emails take. Because a node might wait an arbitrarily long time before forwarding the incoming email this system is primarily meant for non real-time communications. Onion Routing provides a way for two parties - a connection initiator and a connection responder to communicate with each other anonymously. Onion Routing protects its communications against traffic analysis attacks.

It makes it very hard for network observers (such as crackers, companies and governments) to reliably learn who is talking to whom and for what purpose by examining data packets flowing over the network. It concentrates on hiding the source and destination of a packet, rather than the content of the packet. The content of the packet could of course be encrypted using any form of cryptography prior to sending. The system consists of a number of machines, called onion routers. Routers communicate with each other over TCP. Some routers also can serve as entry funnels; they can accept connections from the clients of the network. Some routers can serve as exit funnels; they can create TCP connections leaving the network to the actual Internet services that are being accessed through the Onion Routing network. Such services can be World Wide Web, e-mail, peer-to-peer applications, etc. When a client application wishes to establish an anonymous connection to a server (such that neither the server, nor the network is able to associate the connection with the client), it first of all connects to an application proxy. An application proxy is, for example, a SOCKS proxy that accepts protocol specific connections from applications, and converts them into a generic protocol (such as a stripped down SOCKS protocol). The packets are then forwarded to an onion proxy. The onion proxy creates a route over the onion network and then constructs a special data structure, an onion[3]. An onion is a multiply encrypted layered structure, with information about the route through the network being spread across the layers. The onion is then passed on to an entry funnel. When an entry funnel (or any other onion router) receives an onion, it decrypts it, which reveals a layer containing information about the next hop in the route constructed by the onion proxy. This layer is then stripped off and the onion is forwarded on to this next hop. Eventually, the onion reaches an exit funnel. The decrypted packet is identical to the packet that was produced by the application proxy at the beginning of the connection. This packet will then be sent to the destination TCP host. Onion Routing relies on using Public Key Cryptography, which allows it to encrypt layers of onions such that only.

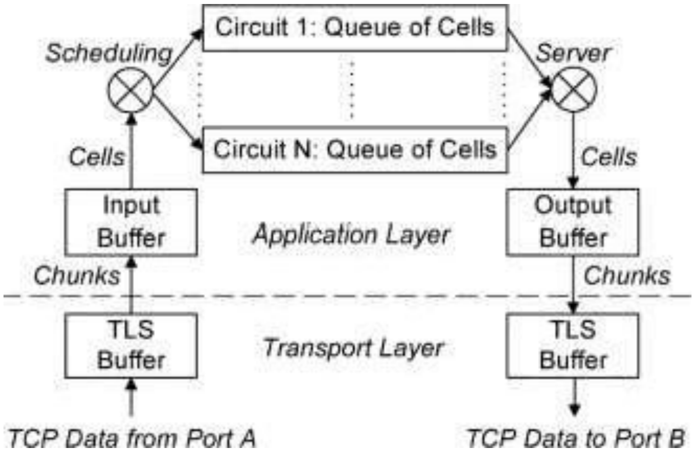

Fig: Processing the cell at onion router

Intended recipients of each layer can decrypt it with their private keys. Each hop along the route then only knows about the previous hop (that it received the onion from) and the next hop (that it was instructed to forward the onion to). Plus, as the entire onion is decrypted at each router, there is no correspondence on the data layer between an onion entering a router and an onion leaving the router. This means that an outside observer who sees the onion for a specific message enter a node does not know which of the onions leaving that node corresponds to that same message. If an eavesdropper compromises a host in the network of onion routers, they will only be able to see where the onion came from on the last hop, and where it should be sent to on the next hop. The absolute source and destination of the onion are hidden[2].

B) Mix Networks And TOR Network:

Mix networks get their security from the mixing done by their component mixes, and may or may not use route unpredictability to enhance security. Onion routing networks primarily get their security from choosing routes that are difficult for the adversary to observe, which for designs deployed to date has meant choosing unpredictable routes through a network. And onion routers typically employ no mixing at all. This gets at the essence of the two even if it is a bit too quick on both sides. Mixes are also usually intended to resist an adversary that can observe all traffic everywhere and in some threat models, to actively change traffic. Onion routing assumes that an adversary who observes both ends of a communication path will completely break the anonymity of its traffic. Thus, onion routing networks are designed to resist a local adversary, one that can only see a subset of the network and the traffic on it[1].

C) Existing Cell Based Attack against TOR

In this[6], firstly we discuss about network components and role of them which process the cell and provide communication between two people.

Step1-Aline(i.., Client): That client always runs a local software called that onion proxy (OP) to anonymize the client data into TOR.

Step2-Bob (i.e., Server): It runs TCP applications such as a Web service.

Step3-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 (512 B) carried through TLS connections.

Step4-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.

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 watermarking 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. In this paper, we focus on the active watermarking technique, which has

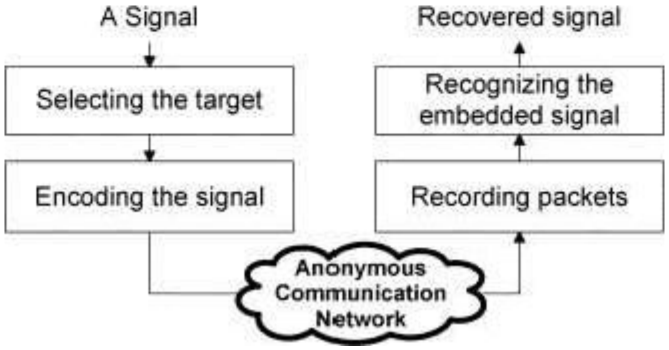

Fig:Cell counting based attack

been active in the past few years. For example, proposed a flow-marking scheme based on the direct sequence spread spectrum (DSSS) technique by utilizing a pseudo-noise (PN) code[4]. 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.

D) Idea Of Cell Base Attack

In the rest of the paper[6], we assume that the attack is initiated at an exit onion router connected to server Bob and intends to confirm that Alice communicates with a known server Bob. An attacker at the exit onion router first selects the target traffic flow between Alice and Bob. The attacker then selects a random signal (e.g., a sequence of binary bits), chooses an appropriate time, and changes the cell count of target traffic based on the selected random signal. As mentioned earlier, when the signal is transmitted through TOR, it will be distorted because of network delay and congestion. For example, when the chunks of three cells for encoding bit "1" arrive at the middle onion router, the first cell will be flushed to the output buffer promptly if there is no data in the output buffer. The subsequent two cells are queued in the circuit queue. When the write event is called, the first cell is sent to the network, while the subsequent two cells are flushed into the output buffer. Therefore, the chunks of the three cells for carrying bit "1" maybe split into two portions. The first portion contains the first cell, and the second portion contains the second and third cell together[5].

When the write event is called, the first cell for carrying the first bit 0 will be written to the network, while the following three cells for carrying the second bit of the signal and one cell for carrying the third bit of the signal will be written to the output buffer all together. When this happens, the original signal will be distorted (i.e., the third bit 0 of the signal will be lost). Therefore, the attacker needs to choose the proper delay interval for transmitting cells[6].

III. SYSTEM IMPLEMENTATION

In this project, we focus on the active watermarking technique, in which as per attacker point of view that changing of data. By interfering with the rate of a suspect senders traffic and marginally changing the traffic rate, the attacker can embed a signal into the target traffic i.e. make changes in the packet arriving at exit router. 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. Our motive behind this project is to detect that particular attacker and as overall analysis it can be concluded that for knowing the services and communication between the users. So while at exit node attacker changes packet data at that time it be get detect by using IP address provided to his computer.

A) Parameters

Sender.
Receiver.
OR Node.
Attacker.
Encryption.

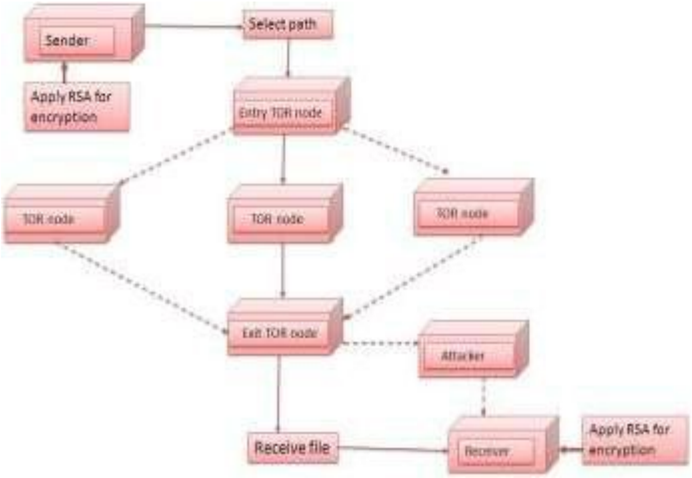

Fig: Block diagram for Anonymity based attack

Decryption.
Port No.
IP Address.

IV. ALGORITHM AND PLATFORM

A) RSA Algorithm

RSA (which stands for Rivest, Shamir and Adleman who first publicly described it), an algorithm for public- key cryptography involves three steps key generation, encryption and decryption. RSA is a block cipher with each block having a binary value less than some number n. That is the block size must be less than or equal to log 2 (n). Encryption and decryption are of the following form, for some plain text block M and cipher text block C:

C = M^e mod n M = C^d mod n

Both sender and receiver must know the value of n. The sender knows the value of e and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = e, n and a private key of PR = d, n. For this algorithm to be satisfactory for public key encryption, the following requirements must meet:

1.It is possible to and values of e, d, n such that M^{ed} = M mod n for all M<n.

2.It is relatively easy to calculate M^e and C^d for all values of M<n.

3.It is infeasible to determine d given e and n.

V. EXTENSION AND MATHEMATIC CALCULATION

A) Impact on controlling both entry and exit onion routers

Attacker needs to set up malicious onion routers in the Tor network. There are four types of onion routers at the Tor network— namely, entry router, middle router, exit router and both entry and exit router (denoted as EE router). In order to understand the impact, we need to evaluate the probability that a TCP stream traverses both the malicious entry onion router and exit onion router. The bandwidth of exit routers is weighted as follows. Assume that the total bandwidth is the total exit bandwidth is B_E. And the total entry bandwidth is B_G. If B_E < (*B*/3), i.e. the bandwidth of exit routers is scarce, the exit routers will not be considered for non exit use. The bandwidth of EE routers are weighted by W_G=1-(*B*/3B_G) where W_G is the bandwidth weight of entry routers an B_G > (*B*/3). If B_G < (*B*/3), then W_G =0.

The probability of selecting the the exit router from the exit set is Bi_E/(B_E+B_{EE} * W_G), where B_{EE} is the total bandwidth of EE routers. Second, the client chooses an appropriate entry onion router OR1 from the set of entry routers, including the pure entry routers and EE routers. To ensure sufficient entry bandwidth, if B_G < (*B*/3), the entry routers will not considered for non entry use. Then, the probability of selecting the *i*th entry router from the entry set is, where W_E=1-(*B*/3B_E) is the exit bandwidth weight and Bi_G is the *i*th bandwidth in the entry set. If B_E < (*B*/3)then W_E =0.

Eventually, the client chooses the middle from the rest of Tor routers. Assume that we configure EC2 nodes as malicious entry, exit, or EE routers. Denote the number of malicious exit routers as, the number of malicious entry routers as , and the number of the malicious EE routers as , where *e3*=*k*-*e*1-*e*2.Based on the above weighted bandwidth selection algorithm, the weight can be derived by Probability can be calculated as follows:

$$
W_{\mathrm{E}} = \begin{cases} 1 - \frac{B}{3\cdot(B_{\mathrm{E}}+B_{\mathrm{EE}}+(e_1+e_3)*b)} : & W_E > 0 \\ 0 : & W_{\mathrm{E}} \leqslant 0 \end{cases}
$$

$$
W_{\mathrm{G}} = \begin{cases} 1 - \frac{B}{3\cdot(B_{\mathrm{G}}+B_{\mathrm{EE}}+(e_2+e_3)*b)} : & W_{\mathrm{G}} > 0 \\ 0 : & W_{\mathrm{G}} \leqslant 0. \end{cases}
$$

$$
\begin{aligned}
P(e) = & \frac{e_1 \cdot b}{B_{\mathrm{E}} + W_{\mathrm{G}} * (B_{\mathrm{EE}} + e_3 \cdot b) + e_1 \cdot b} \\
& \cdot \frac{(W_{\mathrm{E}} \cdot e_3 + e_2) \cdot b}{B_{\mathrm{G}} + W_{\mathrm{E}} * (B_{\mathrm{EE}} + e_3 \cdot b) + e_2 \cdot b} \\
& + \frac{W_{\mathrm{G}} \cdot e_3 \cdot b}{B_{\mathrm{E}} + W_{\mathrm{G}} * (B_{\mathrm{EE}} + e_3 \cdot b) + e_1 \cdot b} \\
& \cdot \frac{(W_{\mathrm{E}} \cdot (e_3 - 1) + e_2) \cdot b}{B_{\mathrm{G}} + W_{\mathrm{E}} * (B_{\mathrm{EE}} + (e_3 - 1) \cdot b) + e_2 \cdot b}.
\end{aligned}
$$

B) Controlling Exit Onion Router

if the attacker does not control entry onion routers the counting attack can be successful. Between entry onion router and client can draw the packets transmitting process. The attacker may recover the signal on the size of packets. In this way, the number of required malicious routers in Tor can also be reduced while the attack still has a desired impact.

C) Attack Detectability

Secret signal which is transmitted by attacker is difficult to detect in the network. That random signal known only to the attacker which is difficult to detect within the target traffic. On the basis of time hopping technique, identification and interception is more reduce the probability of embedded signal.

VI. CONCLUSION

In the TOR network attacker confirms the accurate communication between sender and receiver. Also attacker focuses on targeted traffic and select packet. At exit onion router embedded signals in communication is difficult to detect in the TOR. As given assumption at receiving end attacker get detected by while he/she enters in network with the help of IP address.

VII. REFERENCES

[1] 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.

[2] L. ØVERLIER AND P. SYVERSON, —Locating hidden servers,‖ in Proc. IEEE S&P, May 2006, pp. 100–114.

[3]R. DINGLEDINE, N. MATHEWSON, AND P. SYVERSON,

—Tor: The secondgeneration onion router,‖ in Proc. 13th USENIX Security Symp., Aug. 2004, p. 21.

[4]W. YU, X. FU, S. GRAHAM, D. XUAN, AND W. ZHAO,—DSSS-based flow marking technique for invisible traceback,‖ in Proc. IEEE S&P, May 2007, pp. 18–32.

[5]GURUDAS V. R,‖PREVENTION against new cell counting attack against TOR‖,in Proc international journal in engineering and technology.

[6]WEI YU, XINWEN FU, DONG XUAN, AND WEIJIA JIA,‖ A New Cell-Counting-Based Attack Against Tor‖,in proc IEEE 2012 Transactions on Networking,,volume :pp Issue :99.