Security Issues of Network Mobility (NEMO) with Tor Architecture

Mohd. Altamash Sheikh
Research Scholar,
SOICT, Gautam Buddha University, Gr.Noida India
altsheikh@gmail.com

Abstract— In this paper we discuss NEMO-BSP protocol and TOR architecture. NEMO protocol was initially not designed to handle anonymity of TOR architecture. Due to some of the unique feature of TOR architecture, the use of TOR architecture has been rapidly increased these days. TOR architecture provides anonymity which other network architectures failed to provides. When using a TOR a user feels safe and has no issue of tracking and packet tracing. Therefore whenever a NEMO user uses TOR architecture there are much vulnerability in network. In this paper we outline those security issues in details which arise when a NEMO user uses TOR architecture. We hope in future those issues will be solved and implemented in future so that a user not only remains anonymous while using TOR but also remains secure from various types of vulnerabilities.

Keywords— NEMO, TOR, IPv4, IPv6, MIPv6.

I. INTRODUCTION

We live in a world where security and safety is a topic of great concern, one side we need state of the art security for our devices and on the other side we expect to receive location based services. However we cannot have both the things at the same time full security and location based privacy. There is a need of to make a balance between these two, to get an optimal user experience. Now these days’ internet service providers and search engines like Google are always aware of our location, content we are searching, shopping behavior, banking and expenditure pattern. Companies are working with the objective of maximizing on Profit. The entire framework for user privacy and safety opens an entire new field where there is a lack of rules and regulations from government. This made a user a vulnerable object used by co-operations.

With the facility of mobility user became a mobile internet user, protocols such as NEMO-BSP [1] provides mobility of entire network. Hence this makes system more efficient and most secure because every user don't have true go through the same procedure of handshaking another search procedure which makes them a vulnerability to the network. When there is a compromise of user privacy and location there is a requirement of search an architecture which makes a user anonymous making entire service available to them and remain hidden n the world of internet. One search architecture is known as onion architecture[2]. This architecture provides enormity to a user bye encrypting the entire information into different layers use random path from source to destination. Hence in this way more difficult to trace back a request from server to user because it does not follow direct Path also at each hop route may be altered. Therefore online architecture is relatively a new concept that helps a user to remain anonymous over the internet.

Mobility is always typical to handle, from networking prospective it is not only complicates the system but also adds lots of hardware and software and making it sophisticated system. System which supports mobility most of the time is not a simple one. Radio also supports mobility but it is only a unidirectional system therefore receiver and a sender need not to be synchronized they just transmits the data without any overheads.

A system which have bidirectional communication facility is a complicated one what's lots of synchronization from both the sides there is always hand shake between the parties sending the data in a system like cell phone communication which is also a part of terrestrial communication have a loser always roaming between a certain geographical area therefore they just have to cover the specific area for the coverage hence this does not pose a very serious issues to the designer. What is system like where a user can access anytime anywhere mode this makes is system complicated especially if a user is moving at a very high speed at a very good it height. Like a user travelling inside hey aero plane having all the above discuss characteristics therefore we can apply indoor propagation model form inside the aero plane but however typical outdoor propagation model is not applicable in the case of a aero plane which is moving over the Heights of few kilometers from the Earth surface.

II. NEMO ARCHITECTURE AND WORKING

This section provides a detailed description of the NEMO BSP protocol for providing connectivity to airplane passengers. The architecture of NEMO is almost similar to MIPv6[3]. The architecture consists of Home Agent (HA) which allocates network prefix to all its connected devices.

HA is further connected to Mobile Router (MR), through which all end nodes are connected. All the end nodes are accessible through HA prefix. When an MR is moved to a new location it gets to connect with a new network called Foreign Network (FN) or visiting network. MR moves with all its connected nodes.

Notation	**Description**
NEMO-BSP	Network Mobility Basic Support Protocol
L.E.O	Low Earth Orbit
G.E.O	Geostationary Earth Orbit
M.E.O	Medium Earth Orbit
M.N	Mobile Node
H.A	Home Agent
C.N	Corresponding Node
A.R	Access Router
F.A	Foreign Agent
L.F.N	Local Fixed Node

Now when MR reaches FN it obtains a new address called Care-of address (CoA). After obtaining CoA, MR sends this information of a new address to its HA for updating its cache list called Binding Update (BU). Once HA updates with MR with a new CoA, HA sends an acknowledgment back to MR known as binding Acknowledgement (BA).

Once this procedure is finished, nodes of MR router are reachable to their new address and whenever HA receives any packets it forwards those packets to MR's new location. HA makes a tunnel for sending packets to MR new location.

This method of routing packets from connected nodes to HA and HA to MR is called triangular routing as shown in figure 2, but this method increases the delay of packets as connected nodes are not able to send packets to MR directly. To avoid this, Route Optimization Techniques (ROT) is used which is published in the form of RFC [4]. In ROT connected nodes can send data packets directly to MR and vice versa. In this way, a triangular routing works.

This triangular routing not only simplifies binding procedure but also decreases overall delay. Earlier this was not the part of the original protocol in IPv6[5] but later on, it was updated as an integral part of the protocol.

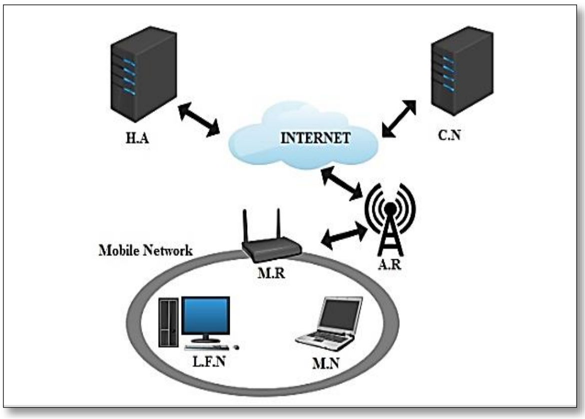

Figure 1 NEMO Architecture

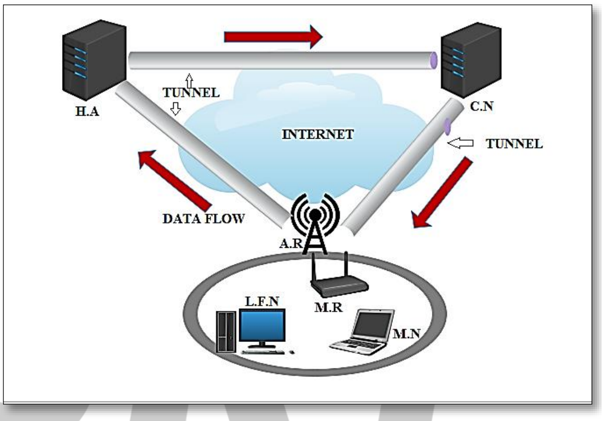

Figure 2 NEMO Triangular Routing

III. UNDERSTANDING TOR

The main objective of TOR is to protect client information protection. The Tor is an abbreviation for the project called "The Onion Router". The Tor was designed for unknown correspondence. The Tor is open source software exist in the form of web browser.

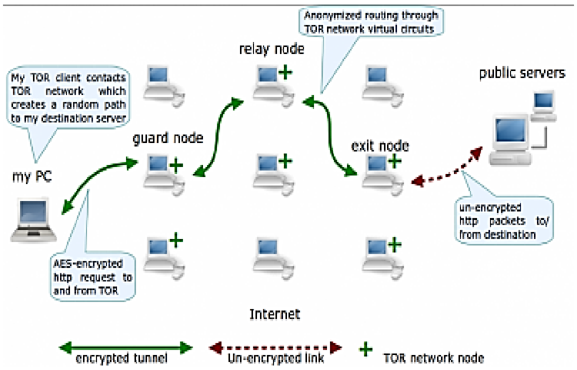
Anonymized routing through TOR network virtual circuits
relay node
My TOR client contacts TOR network which creates a random path to my destination server
public servers
guard node
exit node
my PC
un-encrypted http packets to/ from destination
AES-encrypted http request to and from TOR
Internet
encrypted tunnel
Un-encrypted link
+ TOR network node

Figure 3: working of Onion Routing

The tor diverts internet traffic through a free volunteer overlay system consist of more than 7000 relays. These relays hide user information from anyone who observes network traffic. The TOR do not keep any tracking log of its clients activity. The main focus of TOR is clients security. TOR encryption the information along with next destination IP address, hence a tracker is unable to track source of client or client IP address.

This makes a TOR user secures from back tracking. Some sites however do not allowed access to TOR client into their sites or to their servers. Like Wikipedia do not allowed a TOR user to edit the Wikipedia content. Figure 3 shows the working of TOR architecture in detail.

Authentication: The communications between any two legitimate nodes (e.g., between MR and HA, between MR and CN) must be authenticated, so that no malicious node will be able to generate and send any spoofed packet to a legitimate party.

Authorization: It ensures that only authorized network nodes can be involved in using the network resources or exchanging messages with the network components.

Availability: It ensures that the expected network services are available even if any node is compromised by denial-of-service attack.

Confidentiality: It ensures that the transmitted control packets like (e.g., BU, BAck, dynamic home agent discovery (DHAD) packet, router advertisement) and the data packets cannot be understood by any malicious adversary other than the legitimate recipients.

Location Privacy: This property assures that the actual location of MNNs remain hidden from third parties other than the HA.

Integrity: It assures that the contents of the transmitted messages (like mobile network prefix or source address in BU) from one legitimate party (MR or HA) to other network components (HA or CN) cannot be modified or altered by any malicious intermediate nodes.

Freshness and Anti-replay: This ensures that the control packets (e.g., BU) or data packets sent from the mobile network are recent and fresh. It means no malicious attacker should be able to capture the packets and replay them at a later time.

Robustness against leakage: There are some cases where a cryptographically strong key (generally a private key) has to be stored in tamper resistant modules. Leakage of such keys results in complete breakdown of security of the system. The tamper resistant modules are also not free from bugs and mis-configurations. So the security scheme must provide robustness against leakage of the stored secrets.

Evaluation

In addition to the above security requirements, we suggest the following security metrics to analyze the overall performance of the NEMO security protocols.

Signaling Efficiency: One of the main goals of the security protocols is to keep the signaling overhead as low as possible. A security scheme is said to be efficient in terms of signaling if small number of signaling packets are used.

Delay: The security scheme should not introduce high delay either in the transfer of data or in data processing at any node (CN, HA, or MR). Higher delay will cause the packets at the MRs or HAs to wait for a long time degrading the performance of the protocol

Computational Overhead: Another aim of the security schemes is to reduce the computation burden on the participating entities (HA, CN, MNN, or MR). More computations require more time which ultimately results in longer delay.

Scalability: The security scheme must provide an acceptable level of security even if the network size is increased to a large extent.

Configuration Complexity: This metric indicates that the participating network components need not be equipped with high level configuration for carrying out the desired task. The higher the configuration requirement, the less efficient the security scheme will be in terms of consumption of resources.

Reliability: This metric measures the degree of reliability of the security scheme. The reliability is measured in terms of the strength of the hash function used to calculate the hash digest etc. The more strong the hash function is, the more difficult it will be to regenerate the original message from the hash digest.

IV. SECURITY ISSUES

A. Autonomous system (AS) eavesdropping

If an autonomous system is available on the section ofrelay where client data enters and also at a point where the client exit on the relay then that autonomous system data can be easily statistically vulnerable[6].

B. Exit node eavesdropping

In exit node eavesdropping the vulnerability of TOR is used against itself. As there is no encryption between a server and exit node, therefore any exit node can capture traffic passing through it[7]. A TOR do not use any end to end encryption such as transport layer security (TLS) or secure socket layer.

C. Traffic-examination assault

The traffic examination attack can be done in two separate ways. In first the attacker highlights the traffic from a particular stream from one side and from other side look for the same highlighted traffic stream on the other side of the system. In second method which is dynamic in nature the attacker changes the timings of bundle of the stream as indicated by a particular example and search for that example on the other isde of the system. In this both ways an attacker can connect track a client data and traffic[8].

D. Tor Exit Node Block

Some of the internet users block TOR users to enter into their sites or even restrict use for TOR client[9]. If an internet server is not allowed to track a client they do not allowed client ot use their services like BBC blocks entire traffic form TOR client.

E. Bad Apple Attack

In bad apple attack an attacker is taking advantage of insecure application and TOR design . Whenever a TOR device is taking support from some of the secure application. Hijacker tracks response and control the exit node are some of the common methods used here. This type of attack generally held on P2P file sharing systems[10] as they lacks a secured method for file sharing.

F. Some Protocols Expose Ip Addresses

If a TOR exit node can be controlled, then expose of IP address of a TOR user can also be exposed easily [11].

G. Inspection of Bittorrent Control Messages

Sometimes protocol extension handshakes contain IP address. This may reveals a good amount of information and message of TOR client along with IP address.[12]

H. Hijacking Trackers' Responses

The man in the middle attack is also possible for a TOR client. The communication between a tracker and peer is not authenticated nor encrypted. So if a TOR is used for communication with a tracker directly only than this type of attack is possible [13].

I. Exploiting Distributed Hash Tables (Dht)

A TOR is not able to establish a connection with a distributed hash table easily and hence this attack exploits this weakness. In this way looking to DHT an attacker is able to reveals the target IP address and hence the TOR user security is compromised.

J. Sniper Attack

In this attack an attacker works in association with colluding server and client by over flowing the exit node, until the node is runs out of service and therefore unable to serve genuine clients. In this way an attacker degrades the network performance.

Attacks	**Victims**	**Degree of vulnerability**
Bombing attack	MR, HA, CN	Very severe
Redirection attack	MR, HA, CN	Very severe
Denial of service attack	MR, HA, CN	Very Severe
Replay attack	MR, HA, CN	Severe
Man in the middle attack	MR, HA, CN	Very severe
Home agent poisoning	HA, MR	Severe
Amplification and Reflection attack	MR, CN	Medium

V. CONCLUSION

In this paper we tried to outline the issues of using network mobility with TOR architecture. A NEMO was not initially designed with anonymity hence many of the NEMO procedures get affected by employing TOR architecture. Due to this the NEMO become vulnerable to many security attacks like Eavesdropping, Bad apple attack, Heart bleed bug and Sniper attack.

REFERENCES

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) basic support protocol," RFC 3963, Jan. 2005.

[2] Goldschlag D., Reed M., Syverson P. Onion Routing for Anonymous and Private Internet Connections, Onion Router. (1999.)

[3] Perkins.C et al., "Mobility Support in IPv6",IETF RFC3775,June 2004.

[4] C. Ng, F. Zhao RFC 4889, Network Mobility Route Optimization Solution Space Analysis,July 2007.

[5] S. Deering et al," Internet Protocol, Version 6 (IPv6) " RFC 2460,Dec 1998

[6] Akhoondi, Masoud; Yu, Curtis; Madhyastha, Harsha V. (May 2012). LASTor: A Low-Latency AS-Aware Tor Client (PDF). IEEE Symposium on Security and Privacy. Oakland, USA. Archived

from the original (PDF) on 28 September 2013. Retrieved 28 April 2014.

[7] Zetter, Kim (10 September 2007). "Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise". Wired. Retrieved 16 September 2007.

[8] Soltani, Ramin; Goeckel, Dennis; Towsley, Don; Houmansadr, Amir (27 November 2017). 2017 51st Asilomar Conference on Signals, Systems, and Computers. pp. 258–262.

[9] Zetter, Kim (10 September 2007). "Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise". Wired. Retrieved 16 September 2007.

[10] "BBC iPlayer Help – Why does BBC iPlayer think I'm outside the UK?". www.bbc.co.uk Retrieved 10 September 2017.

[11] Le Blond, Stevens; One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users (PDF). 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11). National Institute for Research in Computer Science and Control. Retrieved 13 April 2011

[12] Manils, Pere; Abdelberri, Chaabane; Le Blond, Stevens; Kaafar, Mohamed Ali; Castelluccia, Claude; Legout, Arnaud; Dabbous, Walid (April 2010). Compromising Tor Anonymity Exploiting P2PInformation Leakage (PDF). 7th USENIX Symposium on Network Design and Implementation.

[13] Jansen, Rob; Tschorsch, Florian; Johnson, Aaron; Scheuermann, Björn (2014). The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network (PDF). 21st Annual Network & Distributed System Security Symposium. Retrieved 28 April 2014.