AN IP TRACEBACK SCHEME FOR SECURING NETWORKS FROM IP SPOOFERS

Prasanthi.L[1], Siva Sravani.K[2], Sruthi.S[3], Swetha.V[4], SELVA KUMAR.A[5]

B.E, (Computer Science and Engineering, T.J.S Engineering College, Tamilnadu, India.

ABSTRACT

In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. The basic protocol for sending data in the Internet network and many other networks is the Internet Protocol ("IP"). The header of each IP packet contains the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. So that the IP Spoofing comes into place. Cloud services offer better options for practical deployment of an IP traceback system. We first present novel cloud-based traceback architecture. We have proposed a novel solution, named Man in the Middle Attack () to avoid the challenges in operation. To capture the origins of IP spoofing traffic is of great importance. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks. Even just approaching the spoofers, for example, determining the ASes or networks they reside in, attackers can be located in a smaller area, and filters can be placed closer to the attacker before attacking traffic get aggregated. The last but not the least, identifying the origins of spoofing traffic can help build a reputation system for ASes, which would be helpful to push the corresponding ISPs to verify IP source address. The proposed solution ensures that the entity requesting for traceback service is an actual recipient of the packets to be traced.

Keyword: - *Networking, Internet Protocol, JAVA, J2EE, JAVA Servlets, My Sql, Modules, Testing, Use Case Diagrams, Net Beans, etc…*

1. INTRODUCTION

Perfect demonstrating and assessment of computer networks rely on the availability of large datasets of Internet flows acquired from backbone links. Those data are needed to support several research tasks, including Internet traffic analysis, modeling of topological distribution, identification of security attacks, and validation of research results. Unfortunately, serious privacy and security concerns discourage the publication of such datasets. On the one hand, network flows carry extremely confidential information that should not be released for privacy reasons. For the sake of this work, we assume that the payload is removed from all packets. However, even in this case, an adversary observing the source and destination IP addresses may associate an individual with the Web sites that she visited, and thus he may infer private information such as political opinions, health issues, or religious belief. Similarly, Internet flows may reveal personal communications among specific individuals, such as e-mail exchanges and chat sessions among them. On the other hand, those datasets may also help an adversary to perform security attacks. For instance, observing the traffic of a target network, an adversary could identify possible bottlenecks to be exploited for denial-of-service (DoS) attacks. For these reasons, several techniques were proposed to sanitize network flows while preserving their utility. Early techniques were based on the substitution of the real IP addresses with pseudo-IDs. However, that method proved to be vulnerable to different kinds of attacks, based on the knowledge of network characteristics, or on the capacity to inject bogus flows in the monitored network. More recently, several techniques have been proposed to avoid the re-identification of IP addresses, based on the perturbation of other fields of the flows. However, those techniques do not provide any formal confidentiality guarantee, and it has been recently shown that they are prone to different kinds of attacks. On the other hand, well-known techniques proposed for micro data anonymization are not directly applicable to network flows, and the

approach of mediated network trace analysis has several shortcomings. Methods for synthetic network flow generation have been also proposed. However, the utility of such datasets was questioned in the literature. In our previous work, we have presented -obfuscation, an obfuscation technique for network flows, which provides formal confidentiality guarantees under realistic assumptions about the adversary's knowledge, while preserving the utility of released data. In that work, we assumed a single release of the whole dataset of flows. However, the incremental release of network flows represents a clear practical advantage. For instance, suppose that an organization wishes to share a month of network flows. Without the incremental release, it would be necessary to wait until the end of the month to start releasing the dataset. Through incremental releases, the organization could provide a timelier sharing of network flows choosing a per-week or even a per-day schedule. Moreover, the incremental release provides important technical advantages. Indeed, the computational costs and the memory requirements for obfuscating a large dataset could be strongly reduced by partitioning the dataset in smaller subsets and by running the obfuscation process independently on each subset. With respect to our previous work, the original contributions of this paper consist in: 1) the identification of confidentiality traces; 2) a novel defense algorithm to apply –obfuscation to incremental releases of network traces; 3) a theoretical proof of the confidentiality guarantees provided by the defense algorithms; 4) an extensive experimental evaluation of the algorithm for incremental -obfuscation, carried out with billions of real flows generated by the border router of a commercial autonomous system.

1.1 Existing System

- Existing trace back mechanisms are either not widely supported by current commodity routers.
- It is very tragic to make Internet service providers (ISPs) collaborate. Since the spoofers are available at every corner of the world, a single Internet Service Protocols to deploy its own trace back system is almost meaningless.
- However, ISPs, which are business entities with competitive relationships, are generally lack in the amount investments which help clients of the others to trace attacker in their managed ASes.
- Since the deployment of traceback mechanisms is not of clear gains but apparently high overhead, to the best knowledge of authors, there has been no deployed Internet-scale IP traceback system till now.

1.2 Objective

In proposed system, we made experiments on traffic diversity, statistical analysis of flow fields, and network flow analysis. Our results show that our technique preserves the data quality in both the single and the incremental release.

2. LITERATURE SURVEY

In this paper, we study the spectrum assignment problem for wireless access networks. We assume that each secondary user will bid a certain value for exclusive usage of some spectrum channels for a certain time period or for a certain time duration. A secondary user may also require the exclusive usage of a subset of channels, or require the exclusive usage of a certain number of channels. Thus, several versions of problems are formulated under various different assumptions. For the majority of problems, we design PTAS or efficient constant-approximation algorithms such that overall profit is maximized. Here, the profit is defined as the total bids of all satisfied secondary users. As a side product of our algorithms, we are able to show that a previously studied Scheduling Split Interval Problem (SSIP) [2], in which each job is composed of t intervals, cannot be approximated within Oðt 1 Þ for any small > 0 unless NP ¼ ZPP. Opportunistic spectrum usage, although a promising technology, could suffer from the selfish behavior of secondary users. In order to improve opportunistic spectrum usage, we then propose to combine the game theory with wireless modeling. We show how to design a truthful mechanism based on all of these algorithms such that the best strategy of each secondary user to maximize its own profit is to truthfully report its actual bid. Auction is widely applied in wireless communication for spectrum allocation. Most of prior works have assumed that all spectrums are identical. In reality, however, spectrums provided by different owners have distinctive characteristics in both special and frequency domains. Spectrum availability also varies in different geo-locations. Furthermore, frequency diversity may cause non-identical conflict relationships among spectrum buyers since different frequencies have distinct communication ranges. Under such a scenario, existing spectrum auction schemes cannot provide truthfulness or efficiency. In this paper, we propose a Truthful double Auction mechanism for Heterogeneous Spectrum, called TAHES, which allows buyers to explicitly express their personalized preferences for heterogeneous spectrums and also addresses the problem of interference graph

variation. We prove that TAHES has nice economic properties including truthfulness, individual rationality and budget balance. Results from extensive simulation studies demonstrate the truthfulness, effectiveness and efficiency of TAHES.

3. PROPOSED SYSTEM

- Instead of proposing another IP traceback mechanism with improved tracking capability, we propose a novel solution, named Man In The Middle Attack (MITA), to bypass the challenges in deployment
- Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding. In such cases, the routers may generate an ICMP error message (named path backscatter) and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers.
- Man in the Middle Attack (MITA) exploits these path backscatter messages to find the location of the spoofers.
- With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks
- The victims can find the locations of the spoofers directly from the attacking traffic

3.1 Advantages of Proposed System

- A practical and effective IP traceback solution based on path backscatter messages, i.e., Man in the Middle Attack (MITA), is proposed.
- MITA bypasses the deployment difficulties of existing IP traceback mechanisms and actually is already in force.
- It may be the most useful traceback mechanism before an AS-level traceback system has been deployed in real to the time till date.

4. RESULT & DISCUSSION

In this project by using application programming interface (API) to track the exact location of the IP address of unauthorized person like hackers, theft etc

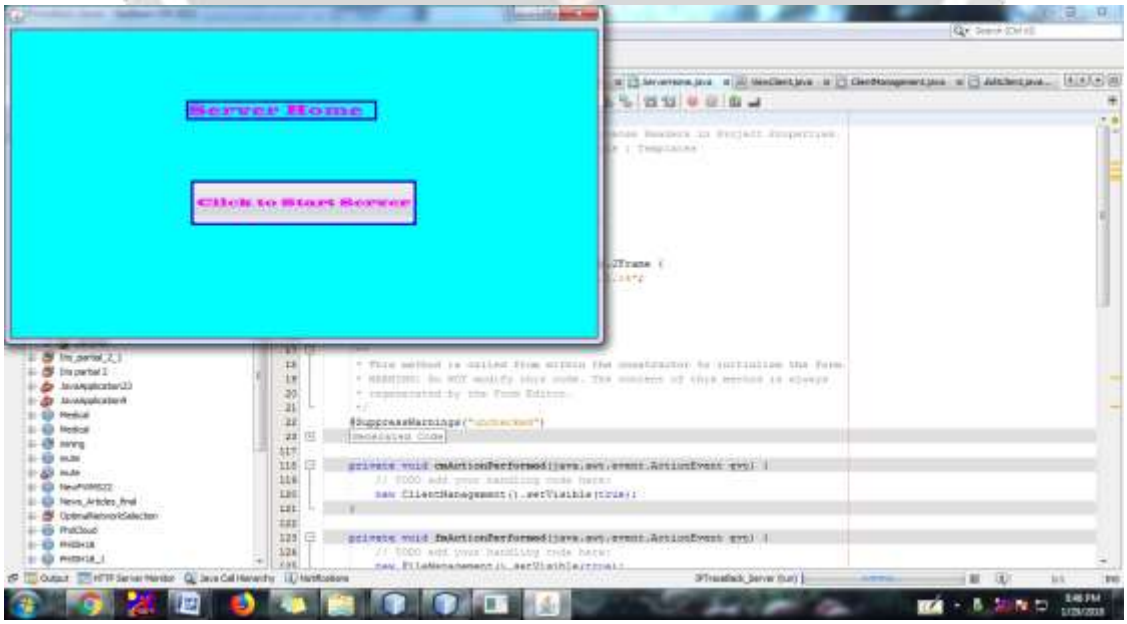

Fig.No.1 Screen Shot of the Project

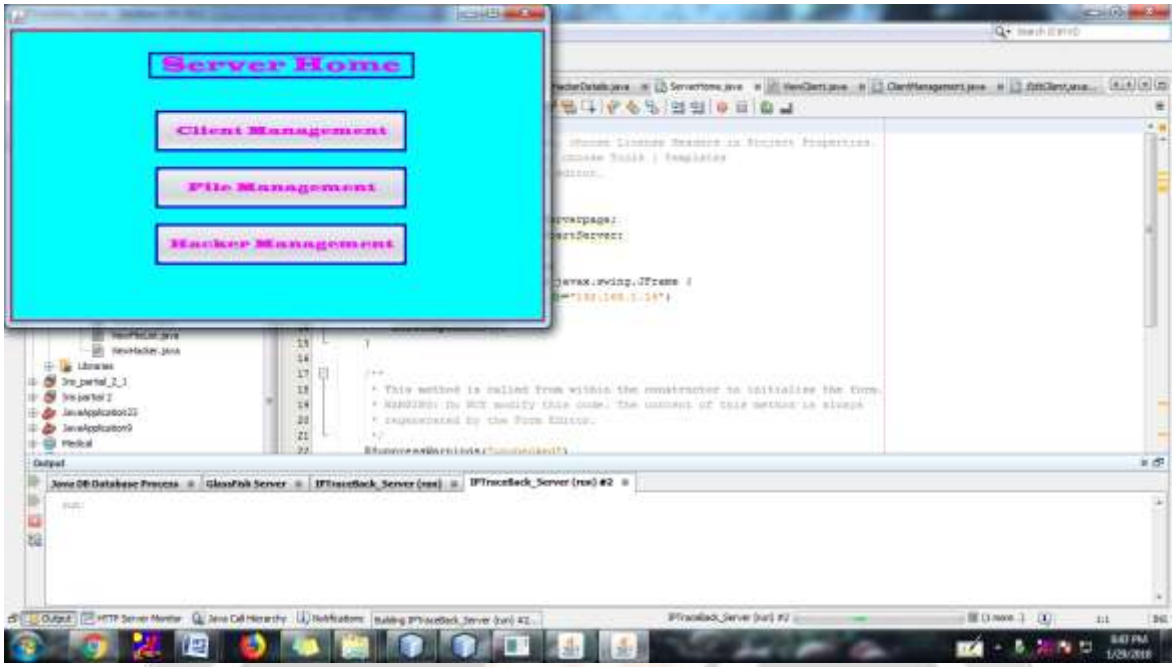

Fig.No.2 Screen Shot of the Project

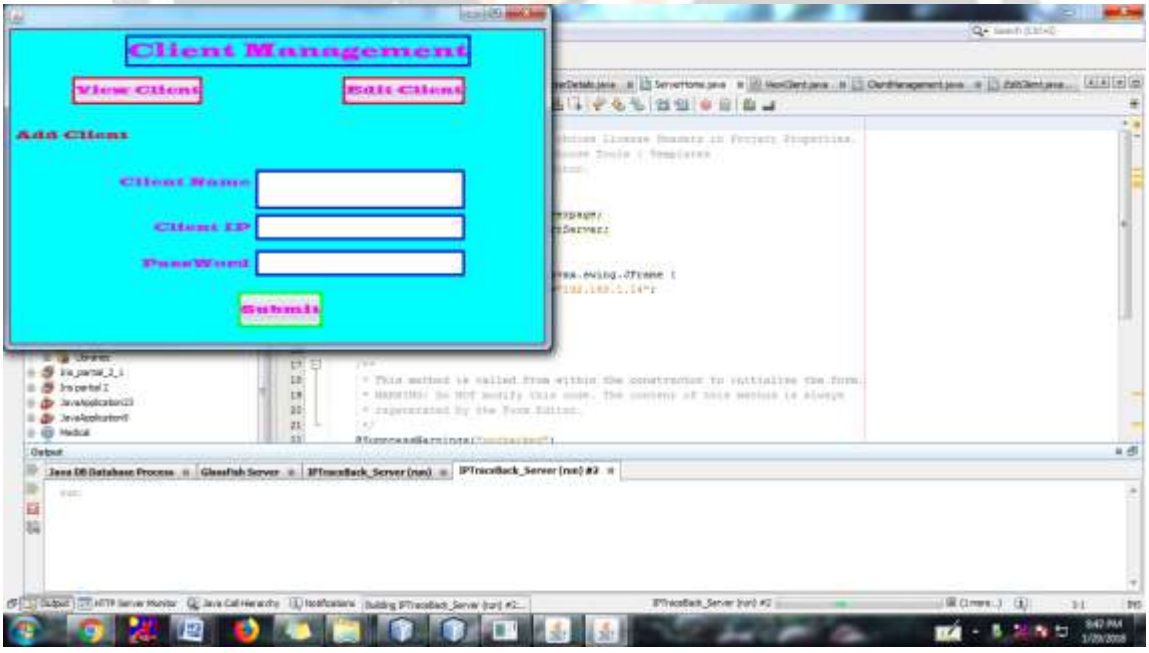

Fig.No.3 Screen Shot of the Project

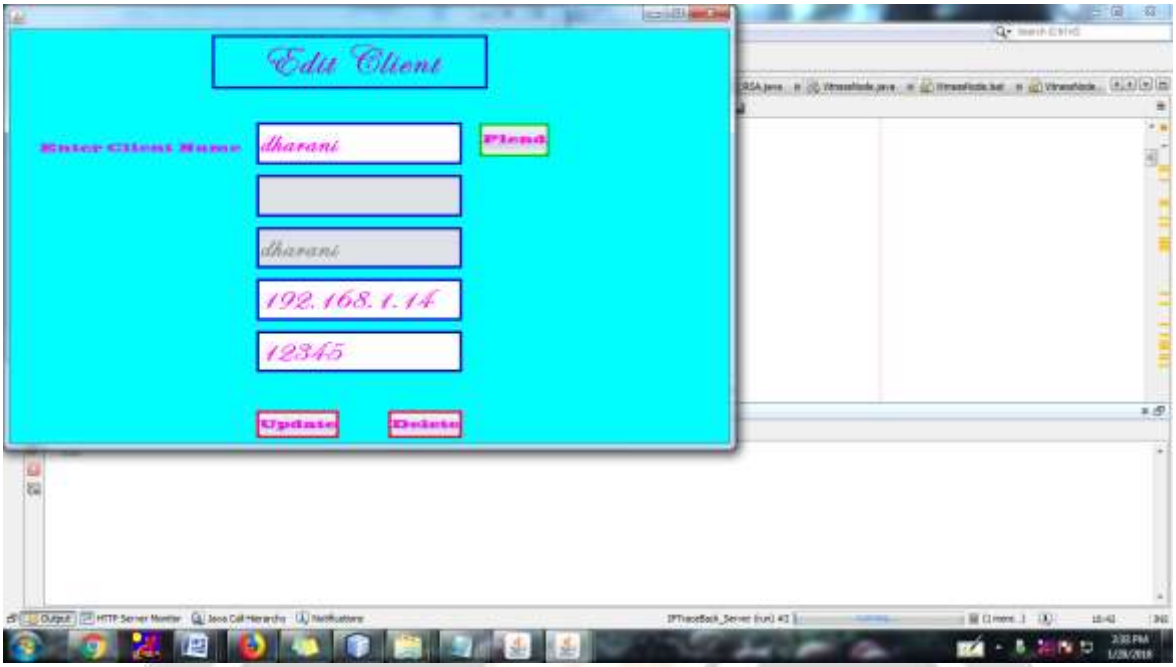

Fig.No.4 Screen Shot of the Project

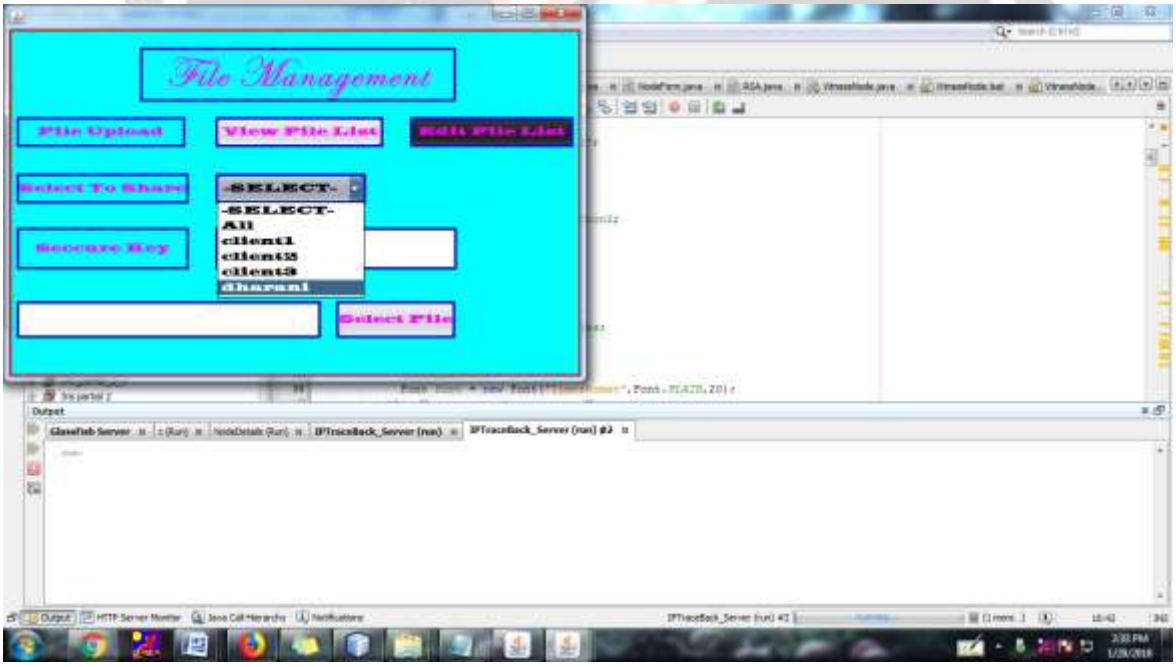

Fig.No.5 Screen Shot of the Project

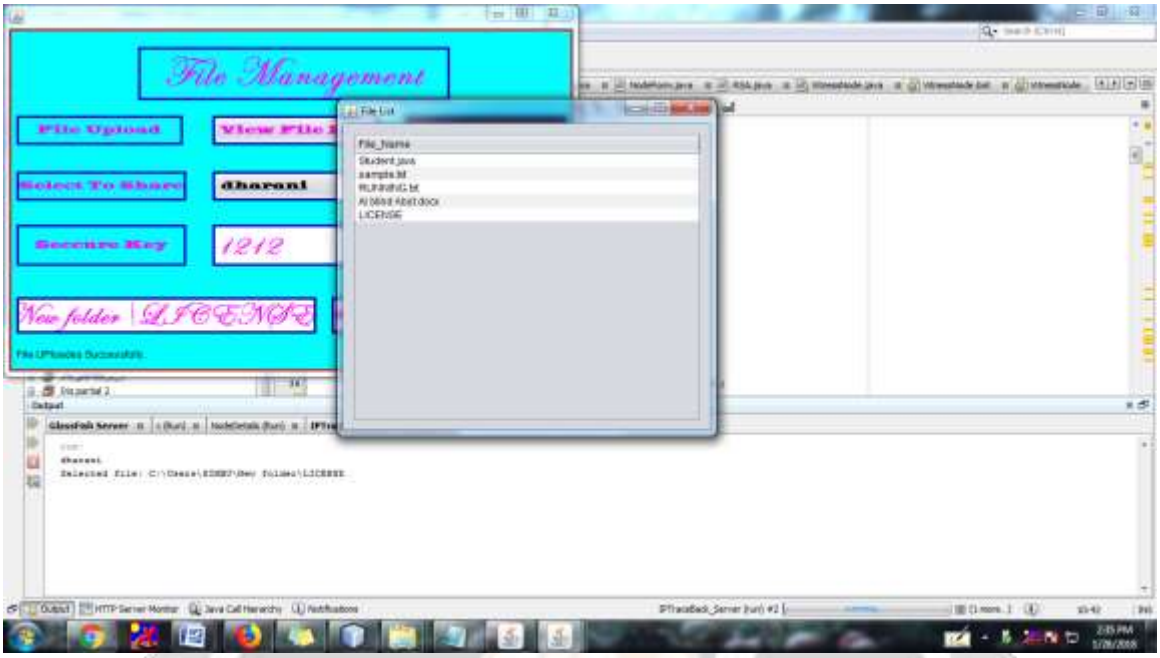

Fig.No.6 Screen Shot of the Project

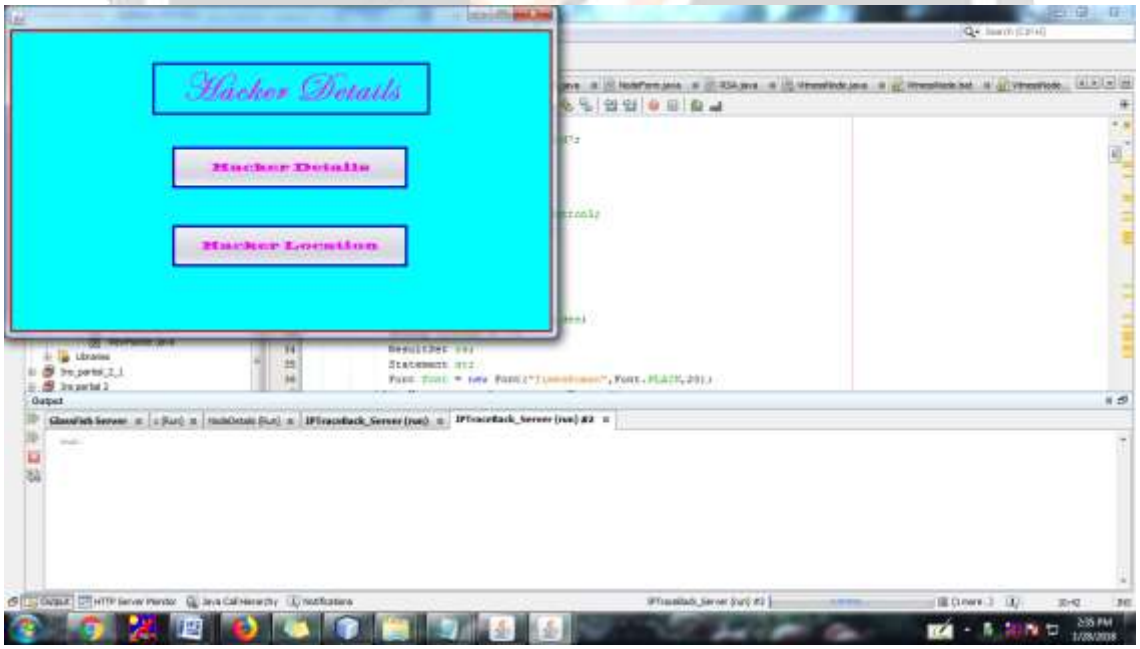

Fig.No.7 Screen Shot of the Project

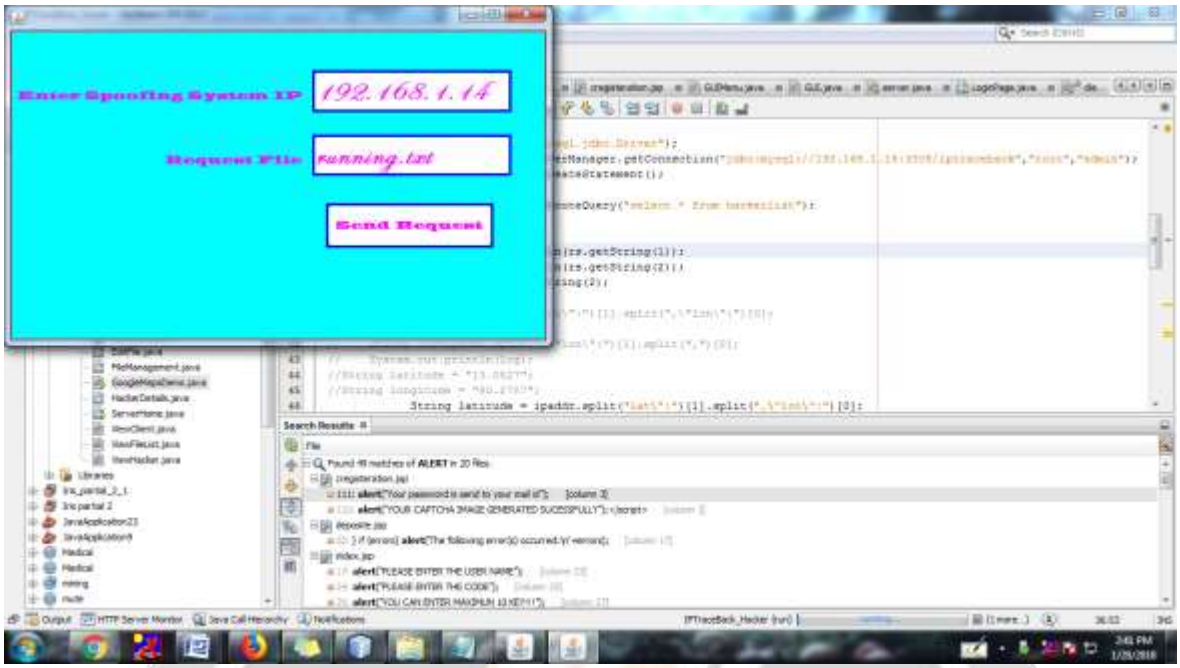

Fig.No.8 Screen Shot of the Project

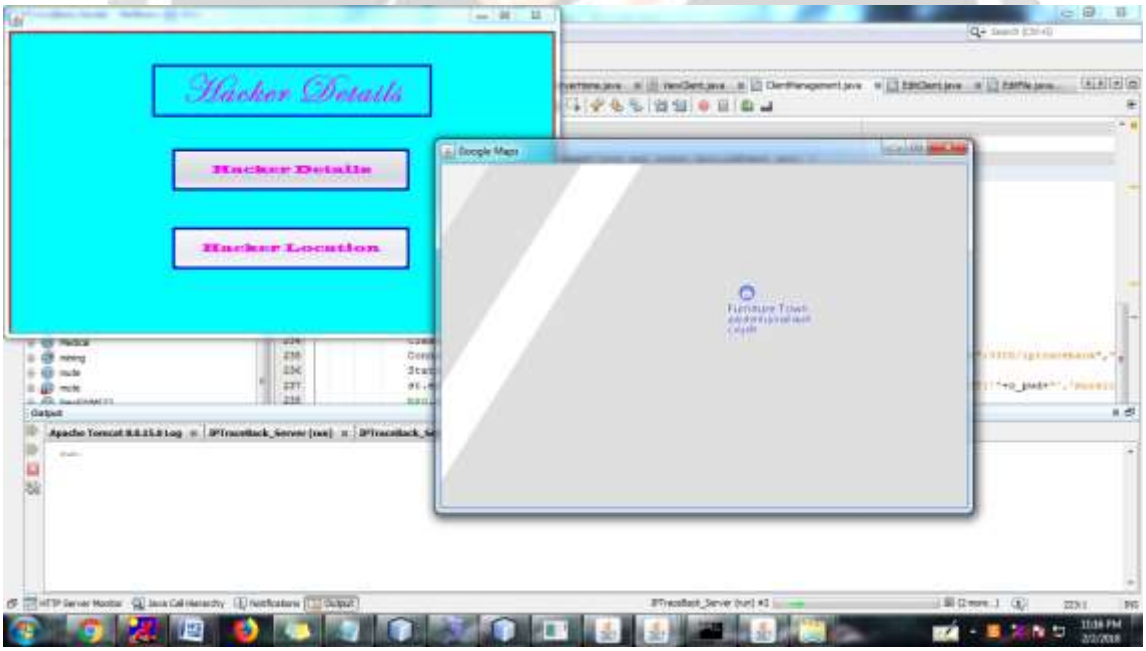

Fig.No.9 Screen Shot of the Project

5. CONCLUSIONS

In this project, we addressed the challenging research issue of network flow obfuscation. We have identified the threats posed by the incremental release of network flows. Based on our previous research, we have proposed a novel algorithm to enforce -obfuscation to incremental releases, and we have formally proved the confidentiality guarantees provided by the new algorithm. We have experimentally evaluated our technique with a very large set of real Cisco Net Flows gathered within an important Tier-II autonomous system. Results showed that our technique preserves the utility of network flows for different network analysis tasks.

6. REFERENCES

[1] P. Xu, X.-Y. Li, and S. Tang, "Efficient and strategyproof spectrum allocations in multichannel wireless networks," IEEE Transactions on Computers, vol. 60, no. 4, pp. 580–593, 2011.
[2] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "TAHES: Truthful double auction for heterogeneous spectrums," IEEE Transactions on Wireless Communications, no. 11, pp. 3076–3080, 2012.
[3] X. Zhou and H. Zheng, "TRUST: A general framework for truthful double spectrum auctions," in Proc. of INFOCOM'09. IEEE, 2009, pp. 999–1007.
[4] S. Wang, P. Xu, X. Xu, S. Tang, X. Li, and X. Liu, "TODA: Truthful online double auction for spectrum allocation in wireless networks," in Proc. of DySPAN'10. IEEE, 2010, pp. 1–10.
[5] P. Xu, X. Xu, S. Tang, and X.-Y. Li, "Truthful online spectrum allocation and auction in multi-channel wireless networks," in Proc. of INFOCOM'11. IEEE, 2011, pp. 26–30
[6] P. Xu, S. Wang, and X.-Y. Li, "SALSA: Strategyproof online spectrum admissions for wireless networks," IEEE Transactions on Computers, vol. 59, no. 12, pp. 1691–1702, 2010.