FACT: A FRAMEWORK FOR AUTHENTICATION IN CLOUD-BASED IP TRACEBACK

K. Gnanalakshmi
M.Phil, Research Scholar, Prist University, Thanjavur, Tamil Nadu, India

G. Gayathri
Assistant Professor, Prist University, Thanjavur, Tamil Nadu, India

ABSTRACT

The main aim of this project is to implement temporal token-based authentication framework for authenticating traceback service queries in cloud-based traceback architecture.

Key word: Traceback, IP address, Cloud Computer. IP traceback


1. INTRODUCTION

IP traceback is an effective solution to identify the sources of packets as well as the paths taken by the packets it can be used for a wide range of practical applications, including network forensics, security auditing, network fault diagnosis, performance testing, and path validation. Many different IP traceback approaches have been proposed, none of them has achieved universal acceptance or practical deployment. The risk of leaking network topology information ranks as the major challenge in hindering the acceptance of traceback techniques. ISPs (Internet Service Providers) are normally reluctant to allow any external party to gain visibility into their internal structure, since such exposure not only leaks sensitive information to their competitors, but also makes their networks vulnerable to attacks. For example, an adversary may misuse traceback services to reconstruct an ISP’s network topology, to avoid this novel cloud-based traceback architecture, to encourage ISPs to deploy traceback services on their networks. While this makes the traceback service more accessible, regulating access to traceback service in a cloud-based architecture.
2. EXISTING SYSTEM
In an existing system traditional logging based traceback traffic digests are assumed to be stored at local router, which is greatly constrained by the limited storage capacity. IP traceback focuses on packet marking based traceback, in marking-based traceback routers add packet tracing information (e.g., router identity) into IP headers to help end-hosts. When sufficient numbers of packets are received at the end-host (victim), the path that the flow of packets has traversed could be reconstructed by the end-host. Essentially, marking-based traceback works fine in partial traceback deployment. Here the term such traceback solutions as end-host centric marking, because the traceback procedure (i.e., path reconstruction) is purely conducted at the end-host. Marking-based traceback was considered to be a promising approach to realize IP traceback, since it imposes relatively little computational and storage overhead on routers.

3. PROBLEM DEFINITION
1. Heavy burden at end-hosts by requiring them to log the received packet-tracing information and then to reconstruct network paths.
2. Performing packet-level logging, however, requires significant storage space and high processing overhead at intermediate routers.

3.1. Proposed System
In our proposed system a novel cloud-based traceback architecture, which exploits increasingly available cloud infrastructures for logging traffic digests, in order to implement traceback. Such cloud-based traceback simplifies the traceback processing and makes traceback service more accessible. A traceback architecture, which possesses several favorable properties encouraging ISPs to deploy traceback services on their networks. Traceback enabled autonomous system (AS) expose their traceback service and traffic flow information collected from routers will be exported to internal cloud storage which is managed by the traceback server in each AS. Here we embed temporal access token in traffic flows and then deliver them to end-hosts in an efficient manner.

4. MODULES
- Network Formation.
- Best Path Finding and Token Generation
- Data Transmission
- IP Trace Back

4.1. Network Formation
Each Autonomous System contains the router and node, autonomous system generates the IP address that respective group of router and node have a same Series of IP address. Each and every AS nodes send route advertisements to the egress routers, and the egress router which is carried out with the eBGP session takes as input all of the route advertisements, each router applies the appropriate import policies before exchanging any iBGP update messages and outputs the set of eBGP learned routes after these import policies have been applied.

4.2. Best Path Finding and Token Generation
The egress routers which are involved in the route selection process select a best route on the basis of certain criteria they are
1) Highest Local preference
2) Lowest as path length
3) Lowest origin type
4) Lowest MED (with same next hop As)
5) eBGP learned over iBGP learned
6) Lowest IGP path s\cost to egress router
7) Lowest Router ID of BGP speaker

For every data transmission source node will send request to trace-back server to generate token for authentication and also key will be generated base on the token for cryptography.

4.3. Data Transmission
In this module source node will send data to destination, data will be transferred through the best path. In this network to provide security data will be transmitted in encrypted format. Here key will be generated based on token. During data transmission trace-back service will be initiated and it will trace the data transmission path and give it to the cloud server. Each and every node details and data transmission details are maintained in cloud server.

4.4. IP Trace Back
In this module the source node transmit data to destination once destination received the data it has to know the data transmission path. So the destination send the request to server with IP address and token (Sequence Number).The server already keeps all the records about the nodes, after destination request received in server it will validate the IP address and token if the IP address and tokens are valid server sends the response as Trace-back IP Path to destination.

5. CONCLUSIONS
Hence we proposed and developed temporal token-based authentication framework for authenticating trace-back service queries in cloud-based trace-back architecture.

5.1. Enhancement
- BGP Network
- Cryptography

5.2. Algorithm Used
- DES
- HMAC
- MD5

REFERENCES


