IP Traceback Technology and its Standardization

Dr. Jianyong Chen
(Vice-Chairman, ITU-T SG17)
(chen.jianyong@zte.com.cn)
ZTE Corporation

2007-04-15

Content

- Definition
- Requirement from Customers
- Current Technologies
- Standardization
- Conclusions

Definition

- The problem of finding the source of a packet is called the IP **Traceback** problem

IP Traceback

- **IP traceback** is a name given to any method for reliably determining the origin of a packet on the Internet

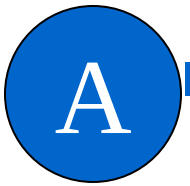
	Social Security	**Network Security**
Protection	No protection [walk on street]	Protection with Firewall etc. [Access to Internet]
Ability of hurt others	Very Easy	Need technical knowledge Something difficulty
Result of hurt others	Criminal	Attacker
Reasons	Law + **strong Traceback ability**	Law + **weak (no) traceback ability**
Expenditure	We needn't buy stronger and stronger armature to protect ourselves	We need buy stronger and stronger firewall and anti-virus software to protect ourselves.
Future	We surely want to continue the approach in **NGS** (Next Generation Society)	Do you think the approach should continue in **NGN**?

Technology

- **Difficulty**
  - IP network is basically stateless
  - Source IP spoofing is rather easy
  - Multi management domains

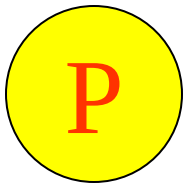
- **Develop from Countering DDoS Attack**

Current Technologies



Active Traceback

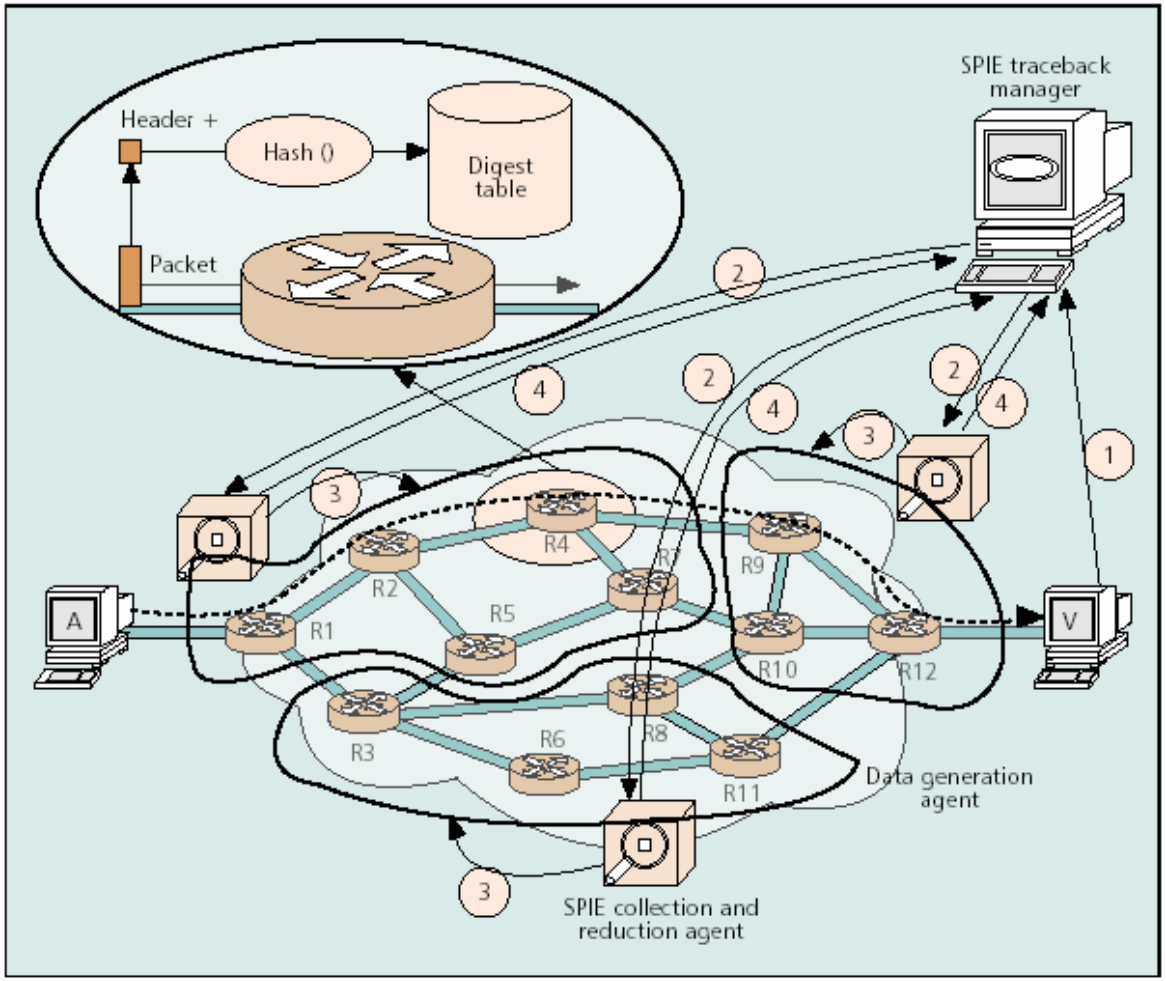
- Router Based Approach
- Packet Marking
  - Probabilistic Packet Marking (PPM)
  - Deterministic Packet marking (DPM)
- ICMP based Approach
- Overlay Network Approach
- Testimony Return Approach



Passive Traceback

- Control flood of link
- IPSEC Based approach
- Ingress filtering

Router Based Approach



Method:

Routers capture every packet with hash(IP header+first 8 bytes of payload)

Deployment:

DGA function of routers store digests.

SCAR-get copies of digests from DGA and reconstruct the path.

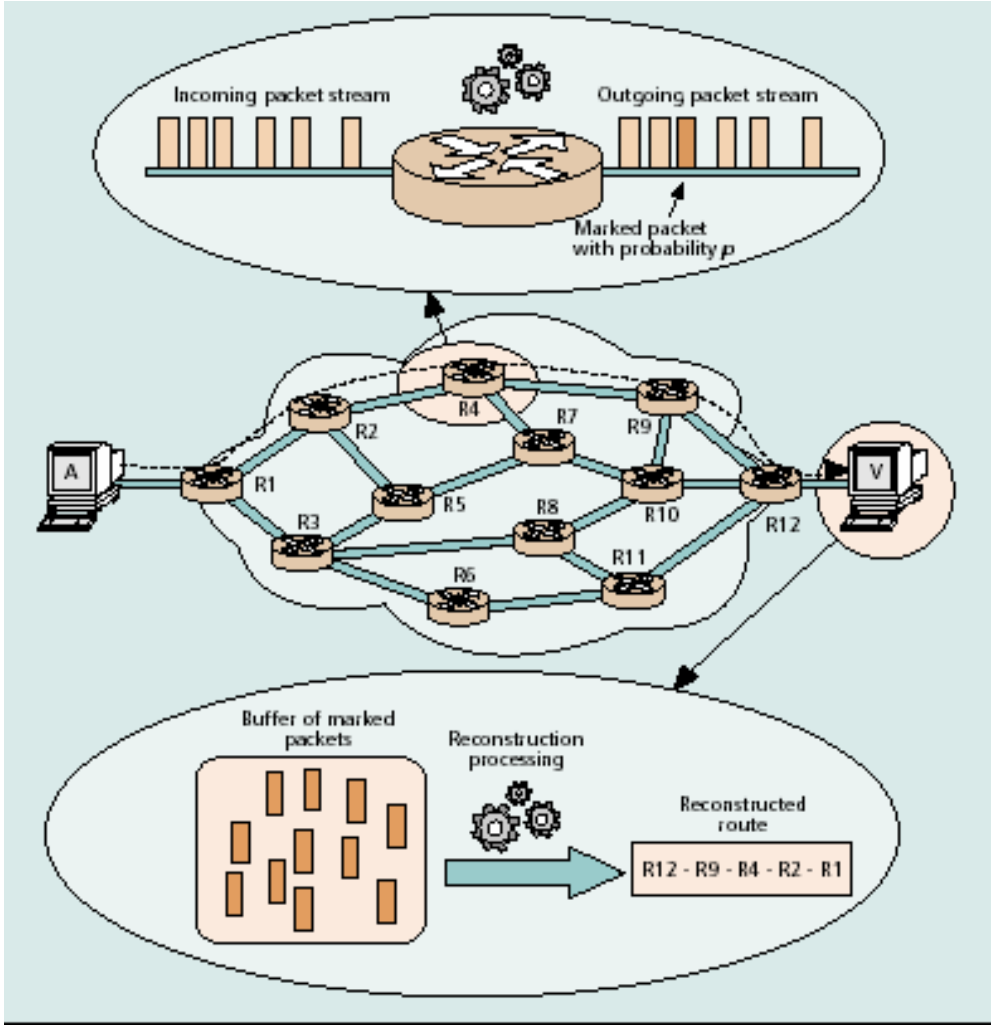
STM-get report and send to Victim

SPIE-Source Path Isolation Engine

- DGA-Data Generation Agent
- SCAR-SPIE Collection and Reduction Agent
- STM-SPIE Traceback Manager

Packet Marking—PPM

(Probabilistic Packet Marking)



Method:

Probabilistically Mark with **Partial address** information of routers

For example:

Mark the package with 1/20,000 probability

Insert 1/K fragment of IP address of router into packet header.

Characteristics:

Fixed space for marking in each packet

Computationally intensive

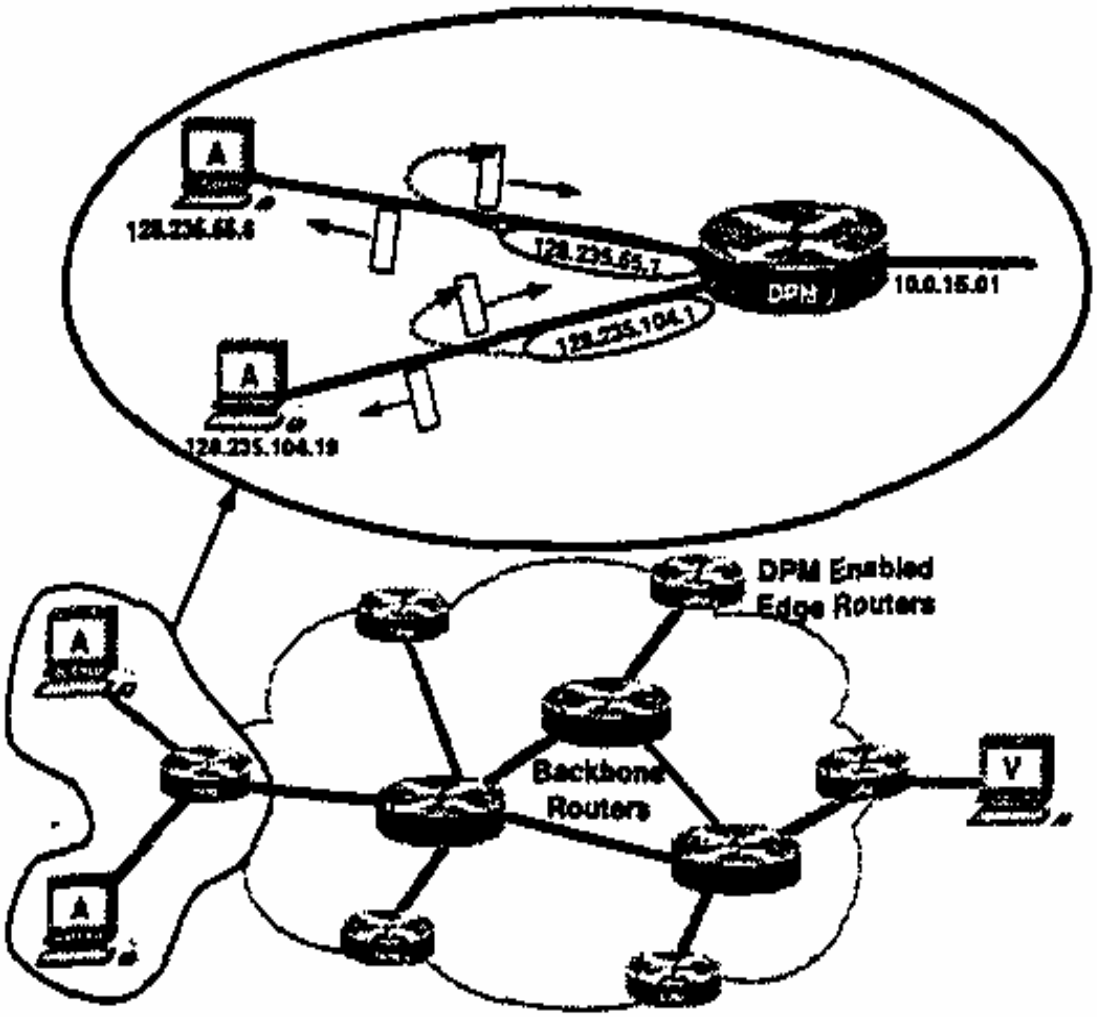
Large false positive

Deployment:

Software upgrade for every routers

Packet Marking-DPM

(Deterministic Packet Marking)



Method

Only Ingress Router mark all the incoming Packets

Where

16 Bit packet ID field + 1 bit Reserved Flag (RF)

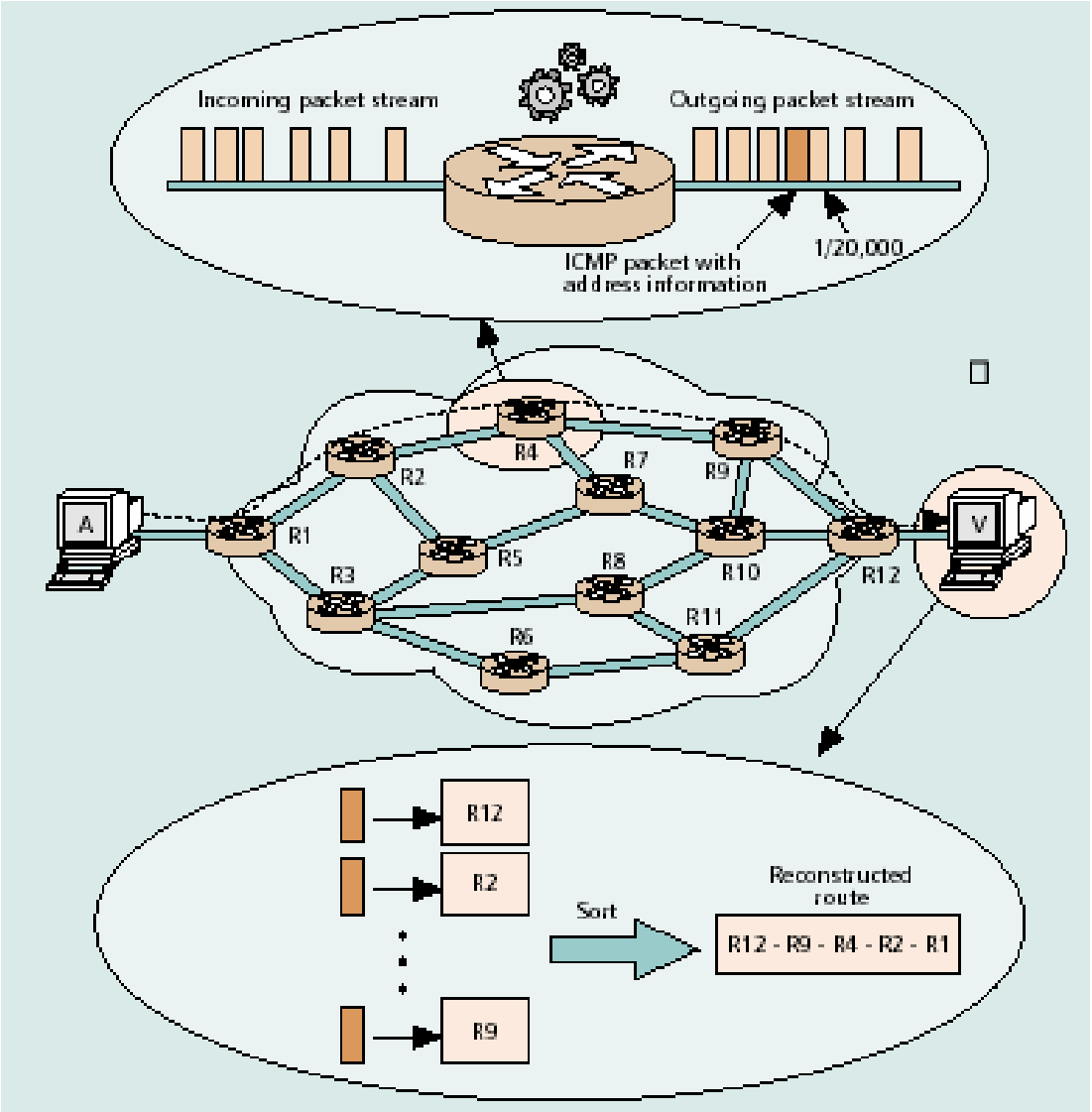
IP address of ingress router is divided into two or more Segments.

Only one of segments is input to the ID field of packet.

Characteristics:

Need table of association between source of attacker and the ingress router

ICMP Based Approach



--iTrace Router

Method:

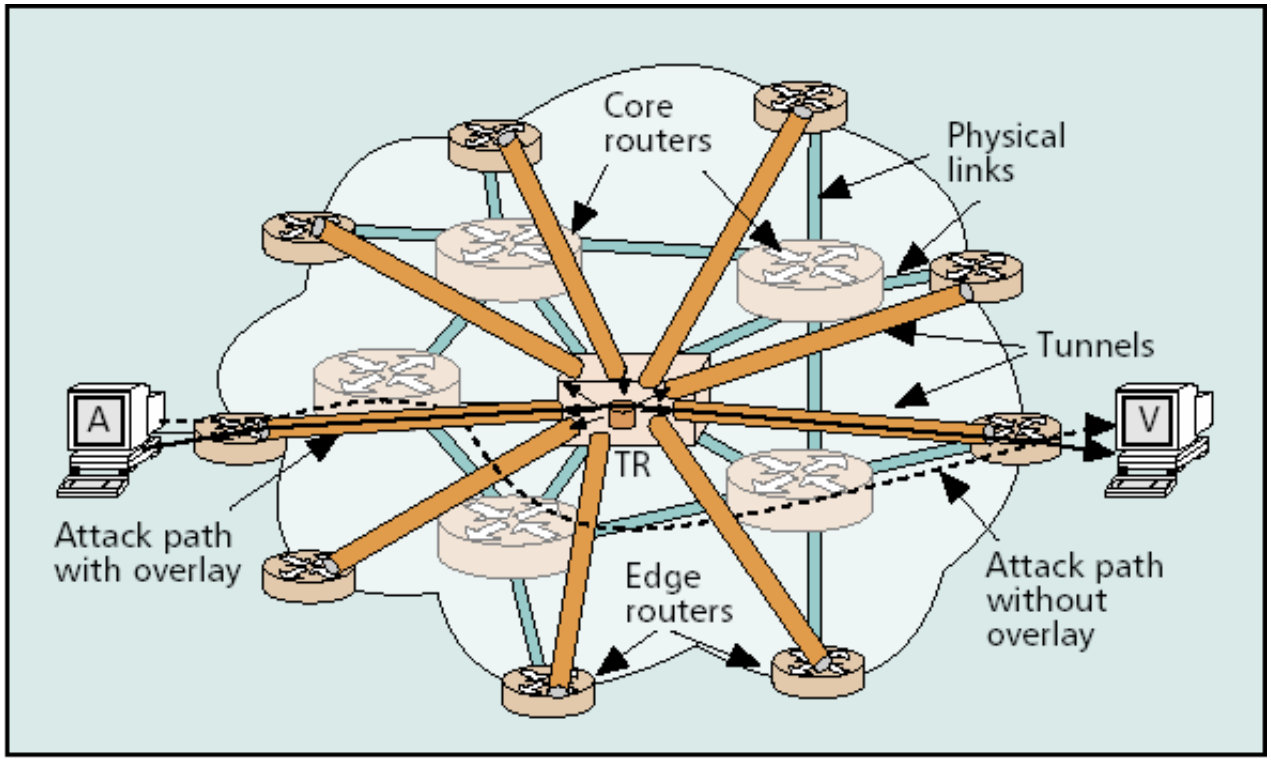
Routers probabilistically sending an ICMP traceback packet forward to the destination of packet.

Characteristics:

Routers commonly block ICMP message because of security.

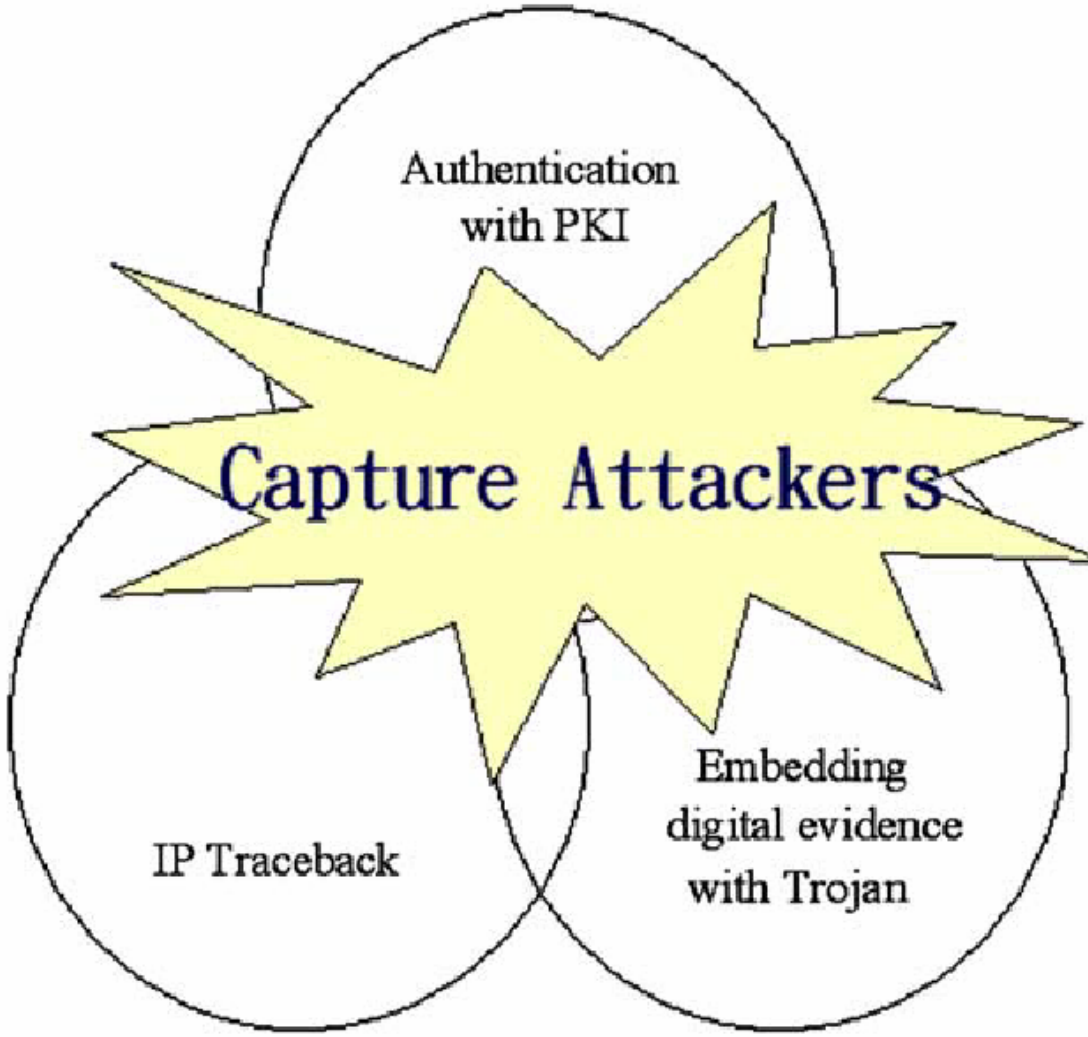
The percentage of ICMP packet near attacker is quite low.

Overlay Network Approach



- Overlay Tracking router (TR) in the network and logically connect to all the edge routers with GRE tunnel
- Generic Route Encapsulation (GRE)
- TR monitor all the packets through the network.
- Difficult to deployment, bandwidth overhead, etc

A Testimony Return Approach



Method:

Authentication center imbed digital evidence with Trojan in ciphertext

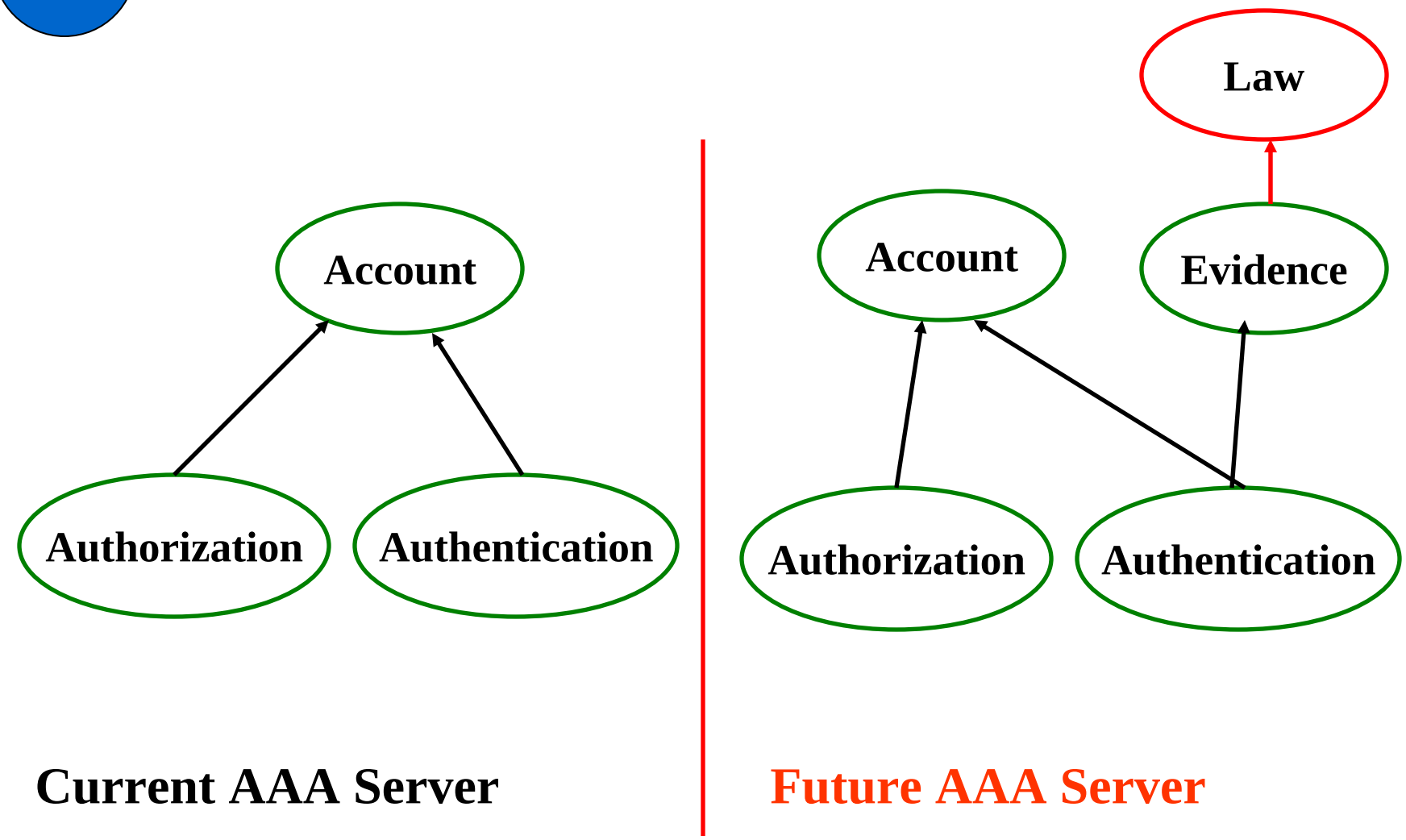
When attacker try to decipher the ciphertext, the trojan is triggered and return digital evidence of computer used by attacker

Drawback:

Trojan itself is an virus.

Attacker decipher the ciphertext offline. This method is fail

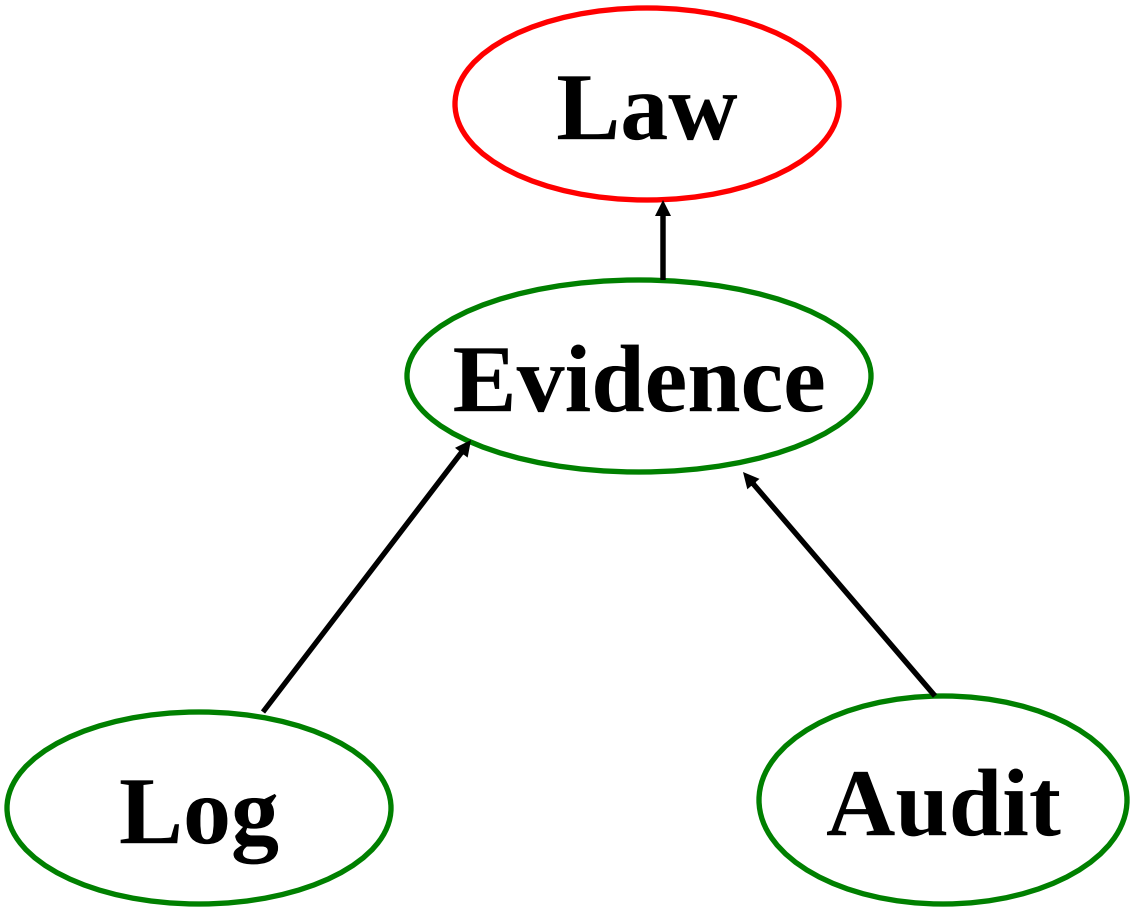
More Traceback-Authentication



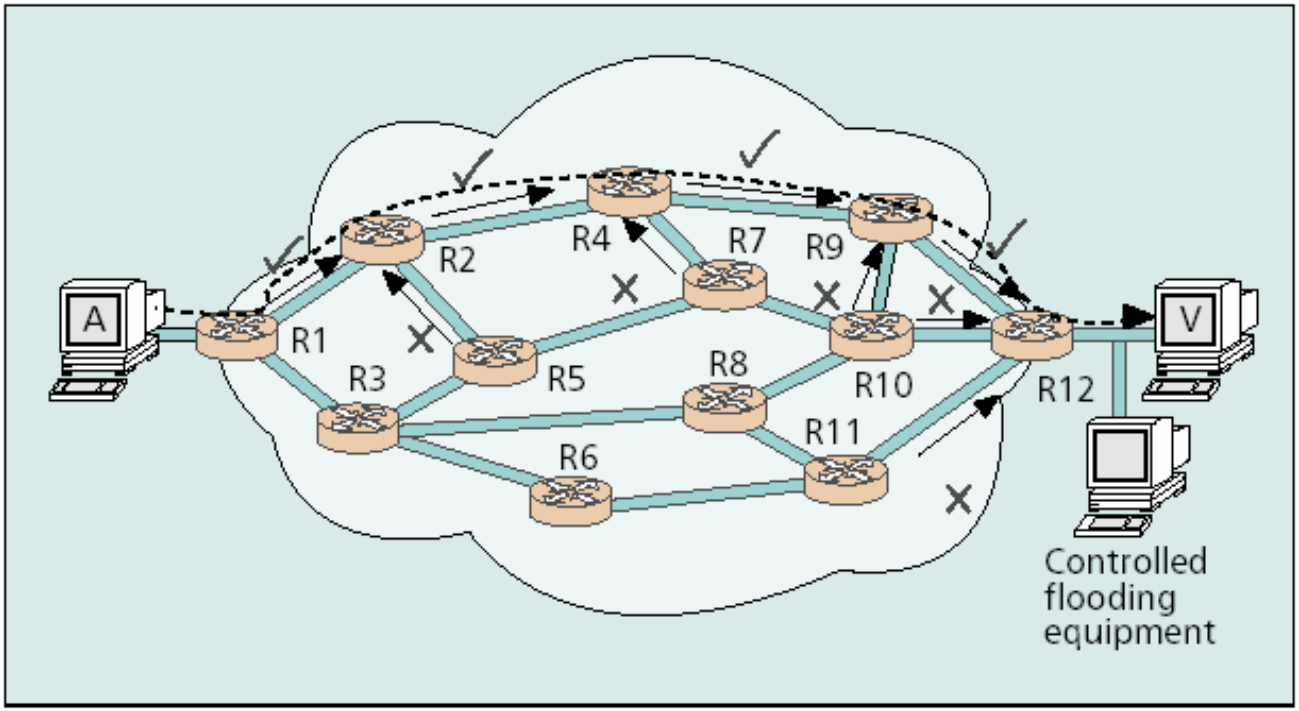
Current AAA Server

Future AAA Server

More Traceback - Log and Audit

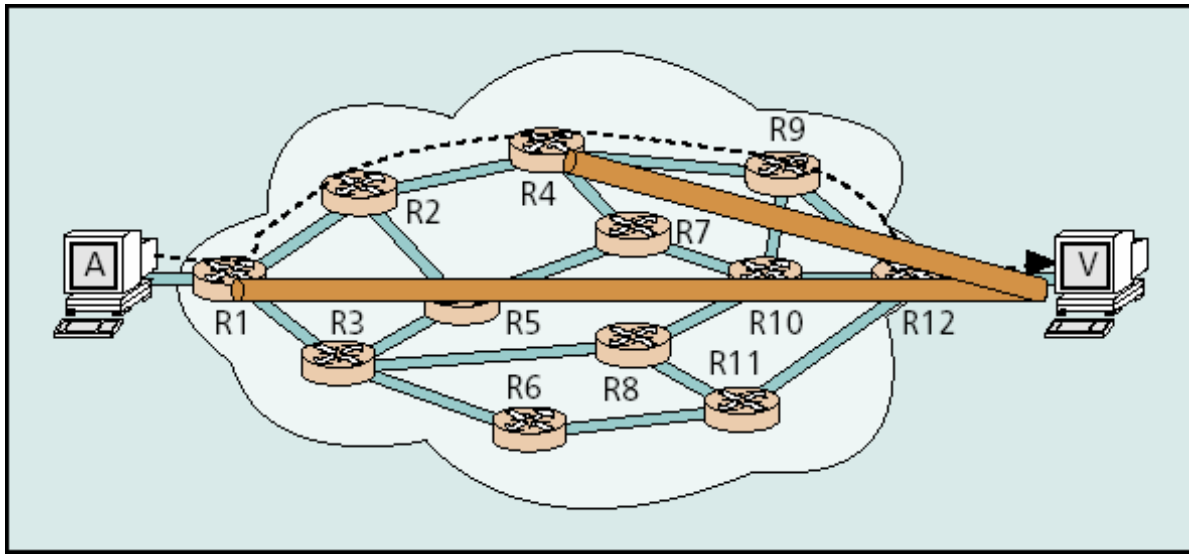


Control Flood of Link

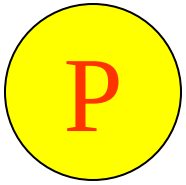


- **Method:**
  - **Test every link hop by hop from the victim to attacker**
  - **Flood a link and cause all packet to be dropped with the same probability. (for example : short burst of traffic from R11 to R12 (X); from R10 to R12 (X); from R9 to R12 (ok))**
  - **If the attack stream drop evidently, then the link is part of he attack path**
- **Characteristics:**
  - **Resource intensive, highly intrusive, only to DoS (not DDoS)**

IPSec Based Approach



- **Assumption**
  - Complete network topology is known
  - IPSec SA between every router and victim
- **Method**
  - According to number of tunnels encapsulating, the attacker is found.
- **Characteristics**
  - Only for DoS attack



Ingress AND Egress Filtering

- **Ingress filtering** -- control the traffic that enters your network and restrict activity to legitimate purposes

- **Egress filtering--** controls the traffic leave your network and restrict activity to legitimate purposes.

- **Characteristics**
  - The simplest and effective mechanism that has been used for many years.
  - Used close to the edge of the network where addressing rules are well defined.

Standardization

iTrace--

- Bellovin S,Leech M,Taylor T.ICMP traceback messages.http://tools.ietf.org/html/draft-ietf-itrace-04
- Withdraw

- **Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing**
  - RFC2827
  - http://www.ietf.org/rfc/rfc2827.txt

Conclusion

- It is necessary to develop traceback technologies as evidence to support law.
  - Current IP traceback technologies focus on DDoS attack.
- It is necessary to develop NGN with strong traceback capability.
  - Current IP traceback Technologies focus on the modification or deployment of current network.
- It is necessary to involve “Traceback Consideration” in developing any new standards
- In terms of security of NGN, Security of our society indicates that it is far more important to depend on **Traceback** than **Protection.**

Thanks

谢 谢

ZTE中兴