

Itrace and the proposal from

Cesar Eduardo Barros

49th IETF - san diego - december 2000

Jerome Etienne

jerome@zeroknowledge.com

Table of content

- **Itrace:** Motivation and principle
 - packet format
 - Attacker model and possible attacks
- **Generation:** Backward itrace: motivation and description
- **Utilization:** mostly authentication
 - possible without a dedicated pki ?
 - with a pki, which authentication ?

Itrace: motivation

- **Goal:** track down the origin of a packet flood
 - Even if the source address is spoofed
 - Currently hard
- **Possible fix:** filter with source addresses on network edges
 - require to properly configure each edge router (rfc2827)
 - infeasible: too many edges

Itrace: principle

- **Principle:** When forwarding a packet, send an ICMP itrace
 - Small probability: $1/20000$ (0.1% of traffic with 20 hops)
 - Tradeoff: most itrace triggered by legitimate traffic
 - waste of bandwidth by sending useless icmp itrace
- **direction:** forward and backward
 - forward: sent toward the destination (original proposal)
 - backward: sent toward the source (cesarb idea)

Packet format: ICMP itrace

- **links**: previous/next hop
 - Information of the neighbors
- **timestamp**: weak way to prevent itrace replay
 - assume a globally synchronized clock
- **Triggering packet**: as much as will fit
- **Authentication**: multiple schemes

Packet format: outer IP header

- **TTL/hop count**: must be set to 255
 - unforgeable minimal distance itrace sender ↔ victim
- **DSCP**: SHOULD be copied from the triggering packet
 - smaller priority → itrace discarded by flood
 - higher priority → itrace becomes a DOS ?

Itrace: Attacks

- **Attacker model:** able to send many packets of any type
 - unable to subvert routers on the path
 - else he would be able to send valid itrace packets
- **Possible attacks:** confuse the victim
 - flood from many small sources
 - send fake itrace

Attacks: small sources

- **principle:** flood from many small sources
 - use each of them below the critical mass
 - impossible to track them down
- **requirement:** high
 - to subvert many sources ?

Attacks: send fake itrace packets

- **Principle:** send fake itrace to confuse the victim
- **spoof a router source address:** may be detected
 - by structural constraints: edge line, ttl
 - by authentication: depend of the chosen scheme
- **use a 'random' one:** easier for the attacker
 - Fake a complete network with valid structural constraints
 - possible only if the victim allows 'holes' in the constraints

Reflectors: principle

- **Definition:** reply to a possibly spoofed source address
 - analyzed by V.Paxson
 - inherent to loosely authenticated datagram networks
- **Example:** any bidirectional protocol
 - TCP, DNS etc... practically all internet servers
- **Several in a row:** *Attacker* → *ref1* → ... → *refn* → *victim*
 - V.Paxson found one: CDN url. negligible?

Reflectors: use by attackers

- **Possible attack:** confuse the victim
 1. flood from a few points
 2. use *many* reflectors as smoke screen
 3. victim must localize the reflectors, then the flood source
- **Efficiency:** very high
 - reflector used below the critical mass (time, packets)
 - victim unable to localize them

Backward itrace: Proposal from Cesarb

- **Definition:** send itrace to the source address too
 - reduce the efficiency of the reflector trick
- **ratio forward/backward:** cesarb proposed 50/50
 - more backward to counter the reflector efficiency ?
- **Limitation:** only one reflector and only at the packet level
 - don't work for the upper layers (e.g. http, recursive DNS)

Itrace: Authentication

- **Goal:** to ensure the received icmp itrace are legitimate
 - the sender is legitimate
 - the itrace generation is legitimate (too hard)
- **sender legitimacy:** two approaches
 1. with a dedicated PKI accessible by victims
 2. no PKI but structural constraints (ttl, edge line)

Authentication: without a dedicated PKI ?

- **without dedicated PKI:** even with perfect authentication
 - only ensure the sender is a computer with a key
 - upper bound
- **Possible enhancements:** impose structural constraints
 1. examples: continuous edge line, ttl trick
 2. less flexible: can cause to discard valid itrace packets

Authentication: Continuous edge line

- **definition:** to receive at least one itrace from each router
- **Continuous edge line:** weak chain of trust
 - itrace packets contain previous/next link
 - assumption: the victim trusts the nearest router
 - is a weak "trust chain"
- weak and moreover hard to obtain...

Authentication: Continuous edge line

- p : prob that a packet triggers itrace (dfl: 1/20000)
- n : the number of packets sent by an attacker
- h : average nb of hops attacker \leftrightarrow victim (dfl: 20)
- l : packet loss ratio router \leftrightarrow victim
 - the victim is flooded \Rightarrow rather high

Authentication: Continuous edge line

- prob for a router to send at least one itrace:
 - $P_{SndLeastOne} = \sum_{t=1}^n \binom{n}{t} p^t (1-p)^{n-t}$
- prob to receive at least one itrace from a router:
 - $P_{RcvLeastOne} = \sum_{t=1}^n \binom{n}{t} p^t (1-p)^{n-t} (1-l^t)$
 - $P_{RcvLeastOne} = 1 - (pl - p + 1)^n$ (← thanks jfr:)
- prob to receive a continuous edge line: $P_{cont} = (P_{RcvLeastOne})^h$

Authentication: Continuous edge line

loss/ P_{cont}	0.05	0.20	0.50	0.80
0.00	39500	51500	68000	90000
0.05	41500	54000	71000	95000
0.20	49500	64000	85000	112000
0.40	66000	86000	113000	150000
0.60	99000	128000	170000	225000
0.80	198000	255000	340000	450000

- **Interpretation:** lack of informations → hard
 - number of packets involved in a Dos ?
 - loss rate close to the victim ?

Authentication: ttl trick

- **TTL**: decremented by each router on the path
- **Unforgeable minimal distance**: if set to 255 by the sender
 - attacker can't pretend to be closer than he really is
 - but can still pretend to be further
- **Assumption**: sent on the path by routers/monitors
 - not by remote boxes receiving flows stats from routers

Authentication: ttl trick usage

- **usage:** unclear
- **principle:** the further the sender is, the easiest it is to fake
 - decrease the trust with the distance ?
- **Evaluation:** depend on the itrace purpose
 - to track down up to the source ?
 - to stop the flood far enough so the victim is unaffected ?

Authentication: with a dedicated PKI ?

- **dedicated PKI**: link all ISPs with a CA hierarchy
 - can ensure the sender is legitimate
- **Disadvantage**: heavier to deploy
- **Trust model**: leaved as an exercise to ISP people :)
 - Hierarchical tree ? ala X509
 - Web of trust ? more flexible and ease the deployment ...

Authentication: draft with a dedicated PKI

- **principle:** avoid any public key operations in routers
 - authenticator = server doing public key ops
 - router ↔ authenticator: shared secret key
 - itrace packets contains the authenticator address
 - verification made between victim ↔ authenticator
- **advantage:** simpler for router
 - less software and CPU usage (no public key)

Authentication:

with or without a dedicated PKI ?

- **dedicated PKI**: stronger and more robust authentication
 - heavier deployment
 - allow remote senders (don't require to modify routers)
- **no dedicated PKI**: weaker authentication
 - structural constraints reduce the problem ? enough ?
 - lighter to deploy

Privacy Issues

- **User:** reveal his location
 - already the case with non-spoofed address
 - legitimate spoofers: mobileIP (only I'm aware of)
 - Mobile users who care can use reverse tunnel (rfc2344)
- **Network:** reveal its topology (more than traceroute?)
 - secret ? security by obscurity ? economic ?
 - Always possible to disable itrace generation

Some open questions

- **Authentication:** is a dedicated pki needed ?
 - are the structural constraints of the nopki scheme enough?
- **Purpose:** what do we want for itrace ?
 - track down up to the source ?
 - just stop the flood far enough not to affect the victim?
- **Limitation:** to force the sender to be on the path, ok ?

Summary: backward itrace

- **Reflectors:** unavoidable
- **Backward itrace:** way to reduce the reflectors trick
- **Questions:**
 - ratio forward/backward ? 50/50 ? more backward ?
 - protocols allowing several reflectors in a row ?
 - only at the packet level is enough ?