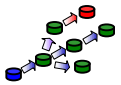


IP TRACEBACK TEAM
NAIST, JAPAN

InterTrack:

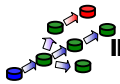
A federation of IP traceback systems across borders of network operation domains

Hiroaki Hazeyama (NAIST)
Youki Kadobayashi (NAIST)
Masafumi Oe (NAOJ)
Ryo Kaizaki (Keio Univ.)

Challenges of attack traceback

- Traceback techniques try to
  - Detect the upstream neighbor routers or ASes of the attack
  - Find the forwarding path of the attack packet / traffic
  - Search the location of attacker nodes or attacker nodes themselves
- Many inter-domain traceback techniques have been proposed such as
  - ICMP traceback message / iTrace
  - Packet Marking
  - Hash digest logging / Hash-based IP traceback

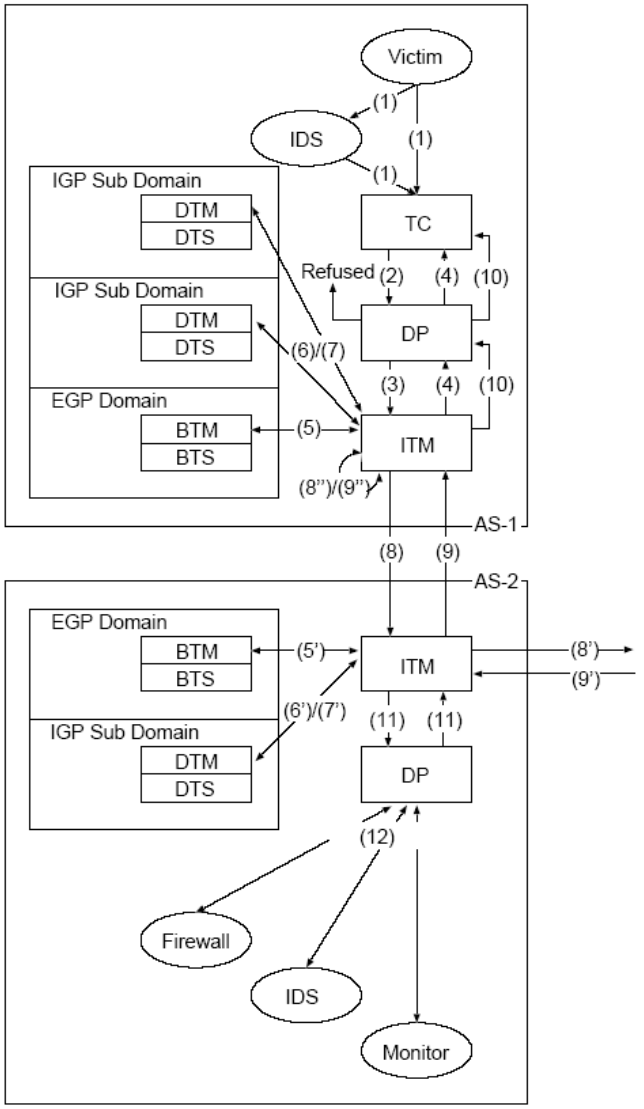
Issues of inter-domain traceback techniques



- The ignorance of network boundaries and the differences of operational policies
  - Existing proposals depend on specific techniques
- The overhead to cooperate tightly with other ASes
  - To collect marked packet
  - To ask further traceback to upstream neighbors
  - To deploy the same traceback technique together
- The risks of depending on one specific technique
  - The dependency cannot avoid evasion attacks
  - The leakage of sensitive information
    - existing proposals might leak the backbone topology

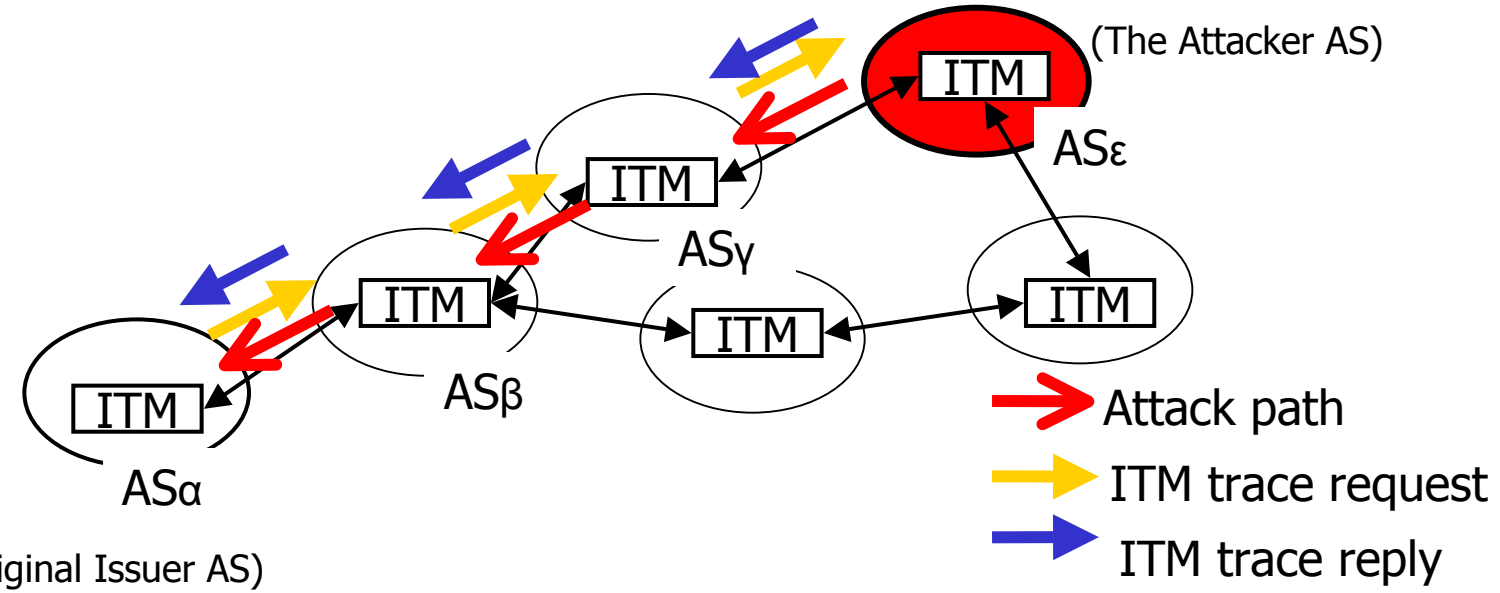
InterTrack approach

- Divide the traceback procedures into 4 level according to the network boundaries
  - Inter-domain : inter-AS tracking
  - EGP domain : border tracking
  - IGP sub-domain : intra-AS tracking
  - Users and operators : tracking initiation
- Use several traceback techniques on border-tracking and on intra-AS tracking
  - Each AS can choose any kind of traceback techniques regardless of other ASes
- Reconstruct the reverse AS path of an attack on inter-AS tracking
  - for loose cooperation among ASes
- Cooperate with detection systems or protection systems
  - for self-defending



Inter-AS tracking

1. Each ITM decides to accept or refuse the ITM trace request along with each AS's policy
2. According to the result of border tracking, each ITM forwards the ITM trace request with adding its AS number to the upstream neighbor AS.
3. Each ITM adds the AS path information into the ITM trace reply message
4. In parallel with inter-AS tracking, ITM on the Attacker AS (AS ε) can start intra-AS tracking



(The original Issuer AS)

Differences from other approaches

- Keep network boundaries on the inter-domain traceback
  - Each AS can operate traceback systems on its own network by only itself
  - Each AS can refuse a traceback requests by its own policy
  - Each AS can trace inside deeply for self-defending in parallel with inter-AS tracking
- Provide independency of specific traceback techniques
  - Each AS can use traceback techniques on its choice regardless of others
- Avoid the risks on inter-domain traceback
  - Each AS can use several traceback techniques both on border tracking and intra-AS tracking
  - Each AS can conceal backbone topology by reporting only AS numbers of up-stream and down-stream neighbors

Prototype implementation

- 50,000 C language codes on FreeBSD
  - Library for basic functions
  - Daemons of ITM and DP
  - A sample BTM / DTM for PAFFI
    - PAFFI : a hash-based IP traceback implementation by Yokogawa Electric Corp.
  - A sample TC using PCAP library
  - InterTrack messages in XML format

```
<?xml version="1.0"?>
<ITMTraceReply>
  <SourceITMID>v4-65002</SourceITMID>
  <Origin>v4-65001</Origin>
  <SequenceNumber>10000</SequenceNumber>
  <TraceResult type="FOUND">
    <ITMSubTrees>                                  // reverse AS path
      <ITMSubTree depth="0" type="FOUND">          // 1st hop result
        <ITMID>v4-65002</ITMID>                    // AS num, protocol
        <NextHops>
          <Incomings>                              // upstream neighbors
            <ITMID>v6-65002</ITMID>
          </Incomings>
          <Outgoings>                              // downstream neighbors
            <ITMID>v4-65001</ITMID>
          </Outgoings>
        </NextHops>
      </ITMSubTree>
      <ITMSubTree depth="1" type="FOUND">          // 2nd hop result
        <ITMID>v6-65002</ITMID>                    // AS num, protocol
        <NextHops>
          <Outgoings>                              // only downstream
            <ITMID>v4-65002</ITMID>                // therefore, attacker AS
          </Outgoings>
        </NextHops>
      </ITMSubTree>
    </ITMSubTrees>
    </TraceResult>
</ITMTraceReply>
```

Current status

- Evaluation
  - Now we are evaluating the prototype implementation in a testbed network composed of 40 blade severs and 4 switches
    - 9 AS (ITM, BTM, BTS), TC, DP
- Development
  - Re-factor for the software release
  - Another sample BTM/DTM implementation
- Cooperation with ISPs in Japan
  - Now we are planning to work together

Summary

- We propose InterTrack
  - As a traceback architecture according to the routing operation
  - As a self-defending architecture to mitigate attacks
- We try to evaluate the prototype implementation
  - on an emulated environment
  - on the real Internet environment

Thank you!

Contact to: traceback@wide.ad.jp

http://member.wide.ad.jp/wg/traceback/index.html

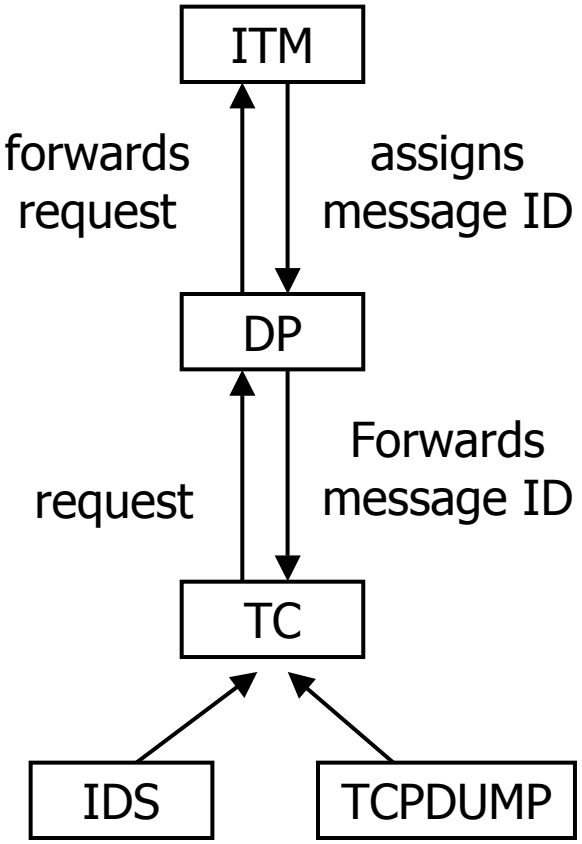
Help slides

Four Tracking Stages

- Tracking Initiation Stage
  - for authenticating clients
- Border Tracking Stage
  - for preliminary investigation inside of each AS
- Inter-AS Tracking Stage
  - for exchanging traceback information among ASes
- Intra-AS Tracking Stage
  - For deep inspection and detecting attacker nodes on the inside of an AS in parallel with the inter-AS tracking stage

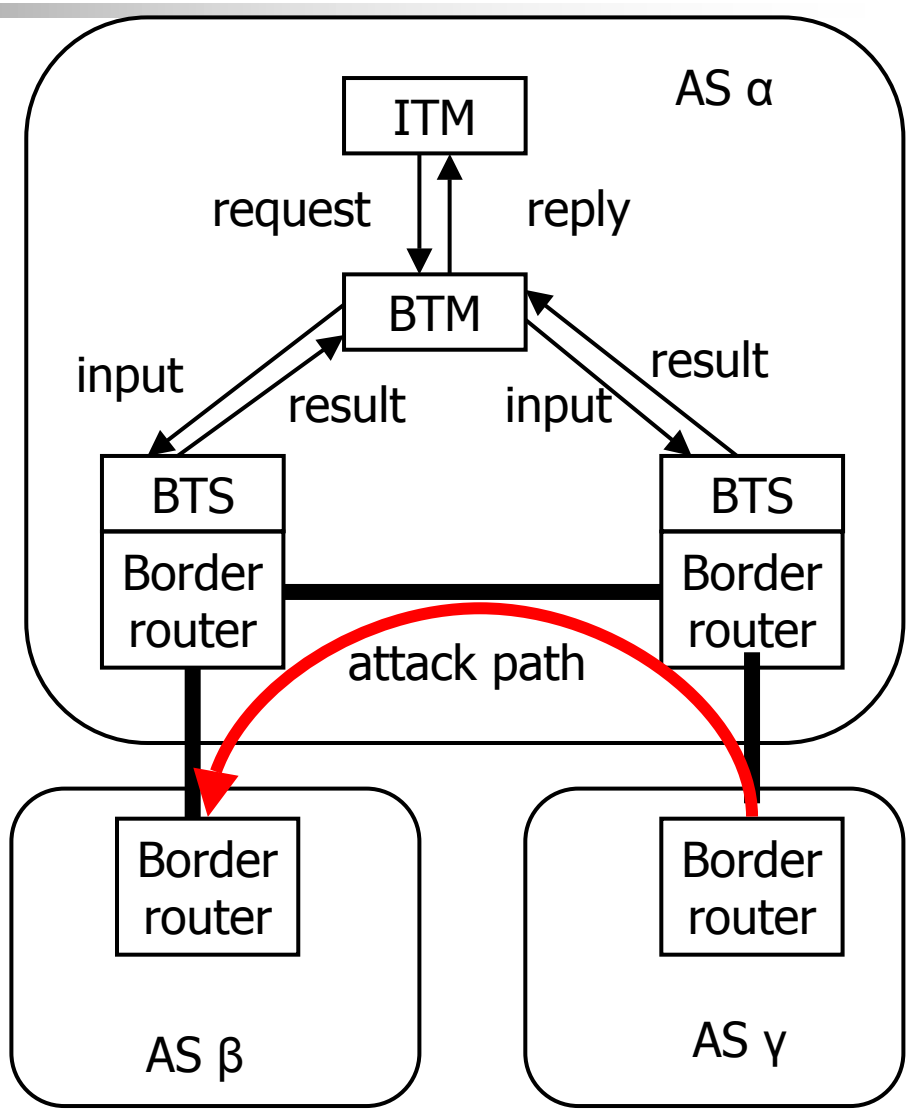
Tracking Initiation Stage

- Inter-domain Tracking Manager (ITM)
  - Mediator of attack traceback among ASes
  - Manager component controls traceback systems on the inside of an AS
- Tracking Client (TC)
  - Wrapper component for detection systems / an operator
- Decision Point (DP)
  - Authenticates TCs and controls the request rates of each TCs



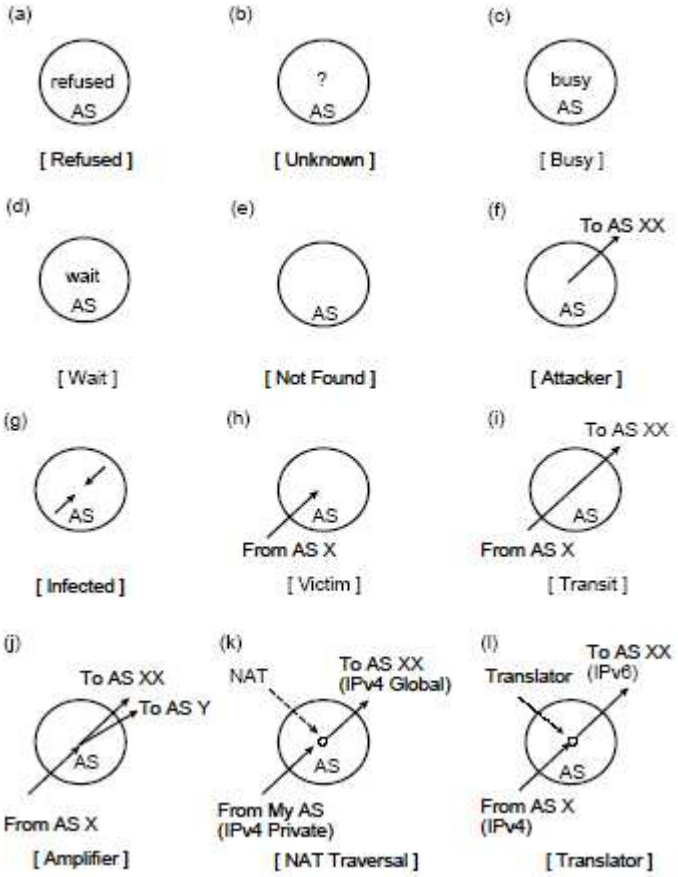
Border Tracking Stage

- Preliminary Investigation on EGP domain level
  - Find the upstream / down stream neighbor ASes
  - Check whether or not it is necessary to inspect the inside of AS more deeply
  - Use several traceback techniques as Border Traceback System (BTS)
    - Hash digest logging
    - ICMP traceback message
    - Remotely triggered blackhole
- ITM kicks the inter-AS tracking stage and the intra-AS tracking stage in parallel according to the result of the border tracking stage



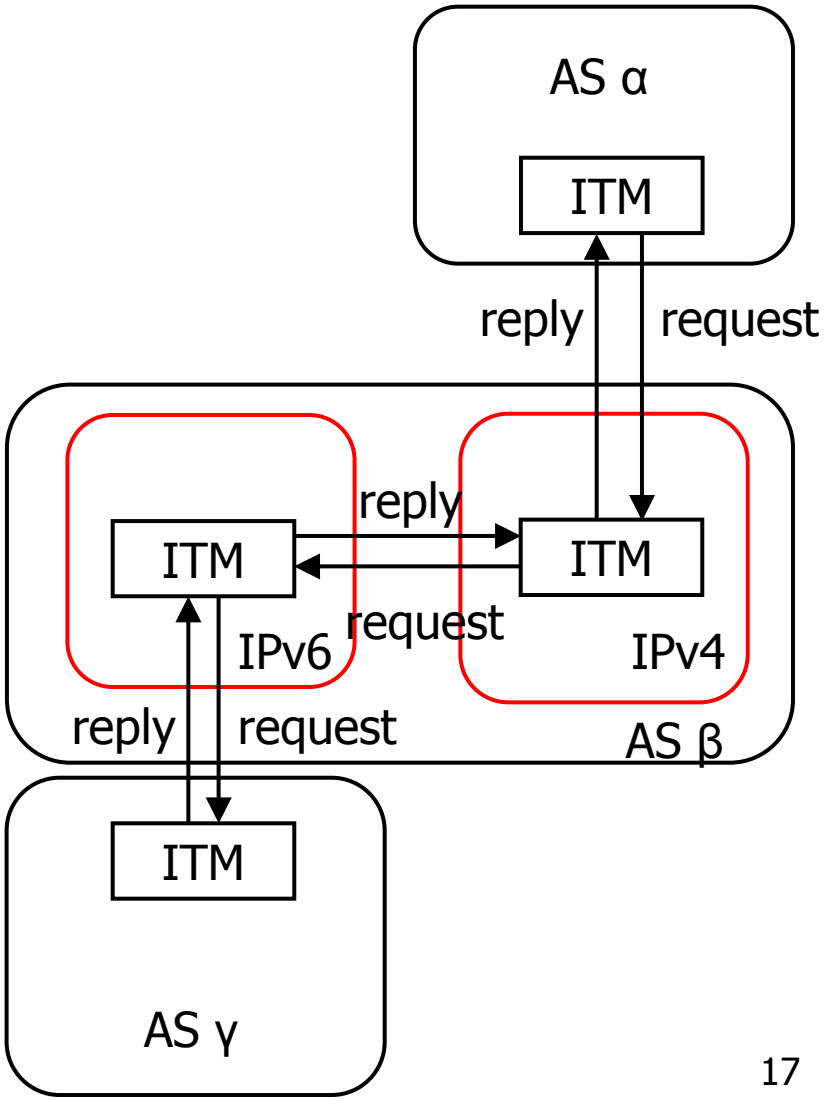
Border Tracking

- Check the AS status and detect the upstream and downstream neighbor ASes
  - Error cases
    - Refused
    - Unknown
    - Busy
    - Wait
  - Basic cases
    - Not Found
    - Attacker
    - Victim
    - Transit
  - Complex cases
    - Infected
    - Amplifier
    - NAT traversal
    - Translator



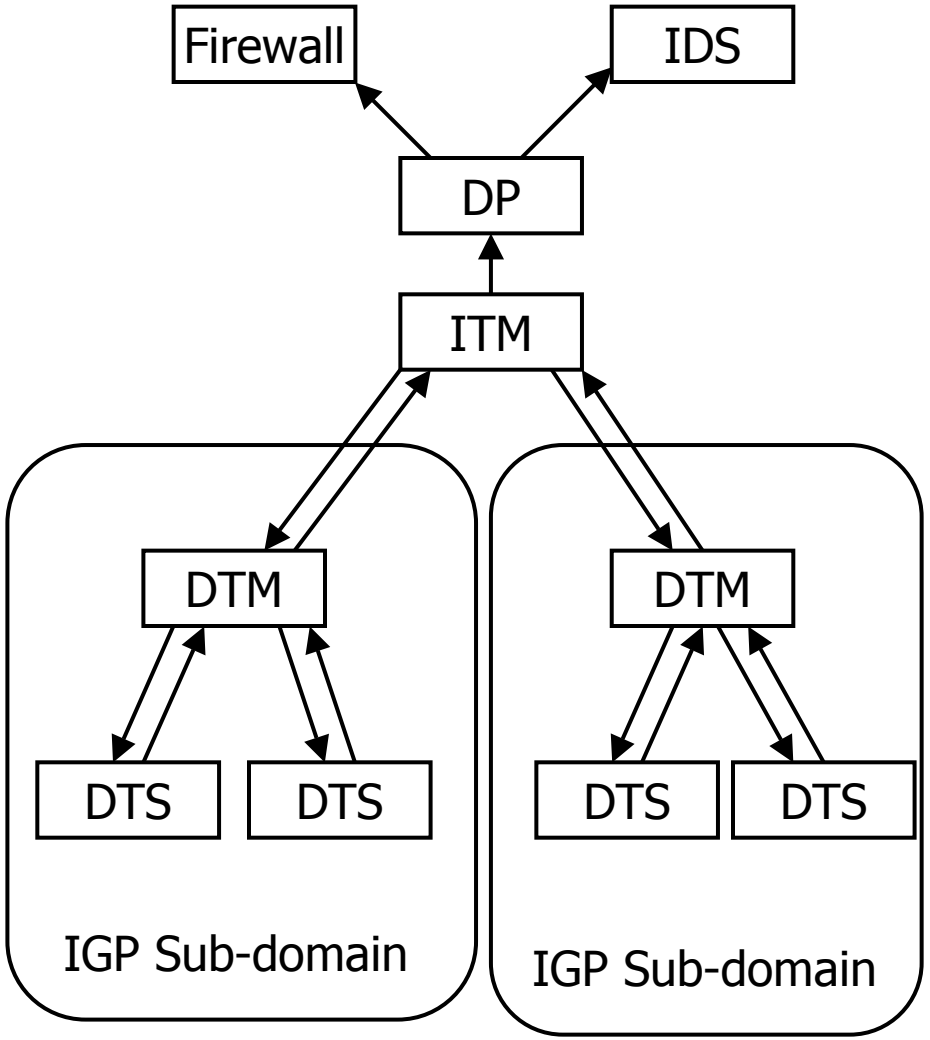
Inter-AS tracking stage

- ITM Forwards the ITM trace request message to upstream neighbor AS
  - From the original issuer AS to the Attacker AS
  - According to the result of the border tracking stage on each AS
- Each AS only adds the upstream / downstream neighbor's AS number into the ITM trace reply message
  - The ITM trace reply message shows the reverse AS path of the attack
- Each AS can refuse to inherit the inter-AS traceback along with its operational policy
- Each AS can start intra-AS tracking in parallel with inter-AS tracking



Intra-AS tracking stage

- For self-defending
  - ITM forward a traceback request to each sub-domain's DTM
  - Each DTM search attacker nodes on the sub-domain
  - ITM aggregates all results from DTMs and store the result to DP of the AS
  - DP exports detection / protection systems for another action



Sample ITM messages

- ITM Trace Request

```
<?xml version="1.0"?>
<ITMTraceRequest>
  <DestinationITMID>v6-65002</DestinationITMID> // receiver
  <Origin>v4-65001</Origin>                     // original issuer
  <SequenceNumber>10000</SequenceNumber>
  <TTL>5</TTL>
  <Footmark transform="yes">
    <PacketDump iftype="0x86">                  // original target packet
      XXXX XXXX XXXX XXXX XXXX XXXX
    </PacketDump>
    <TimeStamp>
      <sec>1132613480</sec>
      <usec>159368</usec></TimeStamp>
    <TransPacket>                               // translate information
      <Border>6TO4</Border>
      <PacketDump iftype="0x86">                // transformed packet
          XXXX XXXX XXXX XXXX
      </PacketDump>
    </TransPacket>
  </Footmark>
  <ITMPathList>                                 // AS path of the request
    <Origin>v4-65001</Origin>                   // original issuer
    <NextHop depth="1">v4-65002</NextHop>       // 1st hop
  </ITMPathList>
</ITMTraceRequest>
```

- ITM Trace Reply

```
<?xml version="1.0"?>
<ITMTraceReply>
  <SourceITMID>v4-65002</SourceITMID>
  <Origin>v4-65001</Origin>
  <SequenceNumber>10000</SequenceNumber>
  <TraceResult type="FOUND">
    <ITMSubTrees>                               // reverse AS path
      <ITMSubTree depth="0" type="FOUND">       // 1st hop result
        <ITMID>v4-65002</ITMID>                 // AS num, protocol
        <NextHops>
          <Incomings>                           // upstream neighbors
            <ITMID>v6-65002</ITMID>
          </Incomings>
          <Outgoings>                           // downstream neighbors
            <ITMID>v4-65001</ITMID>
          </Outgoings>
        </NextHops>
      </ITMSubTree>
      <ITMSubTree depth="1" type="FOUND">       // 2nd hop result
        <ITMID>v6-65002</ITMID>                 // AS num, protocol
        <NextHops>
          <Outgoings>                           // only downstream
            <ITMID>v4-65002</ITMID>             // therefore, attacker AS
          </Outgoings>
        </NextHops>
      </ITMSubTree>
    </ITMSubTrees>
  </TraceResult>
</ITMTraceReply>
```

InterTrack approach

- Divide the investigation level inside each AS to two level along with routing architecture
  - Border tracking level :
    preliminary investigation on EGP domain to find up- / down-stream neighbor ASes
  - Domain tracking level : deep inspection on the IGP sub-domains to detect attacker nodes if needed
- Use several traceback techniques on two tracking level acoording to their characteristics
  - Manager and wrapper module components interconnect different traceback systems
    - ITM : the manager server of an AS
    - BTM : wrapper component for border tracking
    - DTM : wrapper component for domain tracking
- Reconstruct the reverse AS path of an attack
  - Each ITM replies only the results of border tracking on each AS
- Cooperate to detection / protection systems for self-defending
  - TC makes a request from an alert of IDS or a packet dump brought by an operator
  - DP controls request rates from TC and exports traceback results to others