Secure Traceroute to Detect Faulty or Malicious Routing

Venkat Padmanabhan and Dan Simon
Microsoft Research

HotNets-I Workshop
October 2002
Motivation

• Networks are vulnerable to router malfunction
  - faults (bugs, misconfigurations)
  - malicious misbehavior
• What can a malfunctioning router do?
  - compromise routing by fabricating, modifying, or dropping route advertisements
  - disrupt data forwarding by dropping or delaying packets
• This is a problem in various settings
  - Internet
  - P2P/overlay networks
  - multi-hop wireless networks
What can be done about it?

• Flood routing information
  - e.g., sabotage-free routing [Per’88]
  - robust flooding of link-state packets & public keys
  - end hosts construct digitally signed source routes
  - switch to alternate source route upon complaints
  - scaling issues, blind failover could be inefficient

• Authenticate route advertisements
  - e.g., Secure-BGP [KLS’00], SEAD [HJP ’02]
  - prevents spoofing attacks
  - but authenticated info could be wrong...
  - ...and router could drop packets anyway
What can be done about it?

- **Central repository for checking consistency of routing info**
  - e.g., Routing Arbiter (MERIT/ISI)
  - can catch many inadvertent errors
  - but malicious router can still create problems for routes it is “entitled” to advertise
  - ISPs may be reluctant to share policy info
- **Check if packets are forwarded properly**
  - e.g., “watchdog” technique [MGLB’00]
  - assumes that onward transmissions can be heard
  - may not hold even in a wireless setting (for instance, due to directional antennae)
In summary...

• The problem is twofold
  - ensuring the authenticity and consistency of routing info
    • less important when attacks are rare
    • focus of much of the prior work
  - detecting failure of a node to forward packets
    • important when dealing with sophisticated attacks, regardless of their frequency
    • focus of our work
Proposed Approach

• Assumptions
  - single-path routing
  - all nodes are individually globally addressable

• Multiple phases
  - complaint
  - complaint evaluation
  - problem investigation \(\rightarrow\) secure traceroute
  - problem correction
Secure Traceroute

• Normal traceroute useful for identifying bugs or misconfigurations
• But a malicious router could intercept and alter traceroute traffic to give an arbitrary misleading impression
  - it could selectively let traceroute traffic through
  - it could fake responses to frame an innocent router
• Secure traceroute prevents such disruption by
  - verifying the origin of responses
  - validating the correctness of responses
  - preventing special treatment of traceroute traffic
Secure Traceroute Operation

• Tracing can be initiated by any node
• Proceeds hop-by-hop:
  - tracing node establishes secret key with current node
    • ensures secure and authenticated communication
  - tracing node specifies signature of packets to be treated as traceroute packets
  - current node returns “proof” of receipt of traceroute packets
  - current node also returns address of next-hop router
• Two possible outcomes
  - either a complete route is found, or
  - a faulty link is found
R2 initiates secure traceroute

link flagged as faulty

<Check S₃>
<Check S₄>
<Check S₅>

<OK, R₄>
<OK, R₅>

<Not OK>
Authenticating Secure Traceroute

• Need to do a secure key exchange to set up an encrypted and authenticated channel
• Several alternatives:
  - a PKI for routers (as in S-BGP)
  - PGP-style “Web of trust” techniques
  - trusted “key servers”
  - route key exchange via multiple overlay paths
Validating Secure Traceroute Response

• How does traced node prove that it has received the designated traceroute packets?

• Several alternatives:
  - return hash of (certain fields in) all packets
    • no tolerance for packet loss
  - return separate hash for each group of packets
    • probabilistic tolerance for packet loss
  - threshold secret-sharing scheme [Sha’79]
    • allows precise control over tolerance for packet loss
    • but requires packets to be marked
    • quite efficient (e.g., polynomial interpolation)
Using Secure Traceroute

- Complaint
- Complaint evaluation
- Problem investigation
- Problem correction
Complaint & Complaint Evaluation

• Complaint
  - end host experiencing a severe performance problem sets “complaint bit”
  - we assume that spoofing is solved by other means

• Complaint evaluation
  - if complaint level is high enough, a router may choose to investigate
  - best for a router closest to the problem to investigate
  - so each router waits for a random interval based on how far downstream it thinks it is
Investigation

• First do normal traceroute
  - relatively inexpensive
  - effective for the (common) case of failure
• Then do secure traceroute
  - first try to confirm result of normal traceroute by starting with “successful” node closest to destination
  - if normal traceroute found to be misleading, then start at the first downstream node and go all the way
• What if secure traceroute partially deployed?
  - can still identify the subsegment containing the faulty link
Problem Correction

- Corrective action depends on the context
- Several possibilities:
  - route around faulty link
    - source routing makes this easy to do
  - inform a human operator
Impact of Routing Asymmetry

- Impact on end-host complaint process
  - is the problem in the A→B direction, B→A direction, or both?
  - steady stream of bidirectional traffic can help disambiguate unless
    - there is a problem in both direction
    - problem precedes communication between A and B
  - solution: host waits for a random duration and then initiates the complaint process anyway
Impact of Routing Asymmetry

• Impact on secure traceroute
  - makes it hard for investigating router R to check if downstream router D is receiving packets
    • network problems in reverse direction can disrupt key exchange and/or secure traceroute response
  - D can try reverse of forward route to try and reach R
  - in the worst case, R would incorrectly deduce that the problem is at or around D
Attacks on Secure Traceroute

• **Attack**: malicious router can behave correctly when it detects secure traceroute attempts

• **Solution**: simulate secure traceroute activity from time to time

• **Attack**: pair of malicious routers can frame a link in between them
  - upstream one disrupts key exchanges
  - downstream one disrupts traffic

• **Solution**: “onion routing” style encryption of key exchange
blocks key exchange between $R_2$ and $R_5$

falsely suspected link

blocks traffic to $D$
Attacks on Secure Traceroute

- **Attack**: malicious router(s) can lead secure traceroute astray down a path of bogus routers
- **Solution**: persistent application of a succession of secure traceroutes can eliminate bad links one by one
- **Attack**: attacker can generate bogus key exchange messages
- **Solution**: respond to a key exchange message with a “client puzzle”
confederates of $R_4$ or fictitious routers created by $R_4$
Summary

• There are two aspects to routing security
  - securing the routing protocol
  - securing data forwarding
• Secure traceroute enables verification of the correct operation of data forwarding
• Open issues:
  - performance attacks
  - problem correction:
    • similarities to load adaptive routing
  - multi-path routing