Thorsten Strufe

Resilient Networking

Module 3: Routing Security

Disclaimer: This module prepared in cooperation with Mathias Fischer, Michael Roßberg, and Günter Schäfer

Dresden, SS 19
Course Overview

Introduction

Background
- Graphs and graph theory
- Crypto basics (Symmetric/Asymmetric/MACs)

Resilient Routing (Attacks on BGP, SBGP)

IPsec

TLS

DNS Security

DDoS and Countermeasures

Resilient Overlay Networks / Darknets

Intrusion Detection and Response
Module Outline

How does routing work in the first place?

Routing protocols

Threats to routing

Attacks on routing protocols

Defense: S-BGP / SIDR

Pretty good BGP

Topology-based routing security
Recall: 4+ Layers of TCP/IP

End-to-End

Hop-by-Hop

http, ssh, scp, pop3, smtp

Distributed Systems/Applications

http, ssh, scp, pop3, smtp, ...

“Application”

“Transport”

“Internet”

“NW Interface”

App

TCP/UDP

IP

Phys

App

TCP/UDP

IP

Phys

transit network

End-Host

Router

Router

End-Host

http, ssh, scp, pop3, smtp

Distributed Systems/Applications
Who to call, where to send my packet?

Now, how do I find the right cable?

Here: a phone line for each house…
So where do I send this packet?
Who to call, where to send the packet? 😊
And where do I call???

Now, how do I find the right cable?

Here: a phone line for each house...

But computers/servers are much smaller than houses!

One Internet connection per pc? (Don’t forget we’re trying to get IPv6 because we don’t already have enough devices… ;)

So where do I send the packet!?
Can it get worse? :-)

…it can!

But structure helps!?

These examples are already structured!
Network Layer Functions

Transport packet from sending to receiving hosts

Network layer protocols in every host and router

Three important functions:
• Path determination: route taken by packets from source to destination: Routing algorithms
• Forwarding: move packets from router’s input to appropriate router output
• Call setup: some network architectures require router call setup along path before data flows (the Internet does not!)
The Internet Network Layer

No call setup at network layer, no network-level concept of “connection”

Routers do not process or store state about end-to-end connections

Packets are typically routed using destination host ID

Packets between same source-destination pair may take different paths
# Internet Names and Addresses

<table>
<thead>
<tr>
<th></th>
<th>Example</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td><a href="http://www.ietf.org">www.ietf.org</a></td>
<td>hierarchical</td>
</tr>
<tr>
<td>IP address</td>
<td>132.151.1.35</td>
<td>topological (mostly)</td>
</tr>
<tr>
<td>MAC address</td>
<td>8:0:20:72:93:18</td>
<td>flat, permanent</td>
</tr>
</tbody>
</table>

**DNS**
- many-to-many

**ARP**
- 1-to-1

**Host Name** ➔ **IP Address** ➔ **MAC Address**
IP Addressing (1)

IP Address:
32/128-bit identifier for host or router interface

Interface:
Connection between host, router and physical link
- Router’s typically have multiple interfaces
- Host may have multiple interfaces
- IP addresses associated with interface, not host or router

223.1.1.1 = 11011111 00000001 00000001 00000001
223 1 1 1
What Happens in the Routers?

- Intermediate Systems (routers) on the Internet have two main functions
- Routing: Determine which route to use
- Forwarding: What happens when a packet arrives?

![Diagram showing routing and forwarding processes.]
General Threats to Routing Protocols

Threats to routing can be characterized according to:

— Threat source:
  — Subverted link or subverted / rogue router

— Threat consequence (generic):
  — Disclosure of (routing) information
  — Deception of other routers (e.g. with forged messages)
  — Disruption of normal (router) operation
  — Usurpation (= gaining control over a routers operation, e.g. by “stealing” traffic originally to be routed by that router)

— Threat consequence zone:
  — Single node / part of a network / whole Internet

— Threat consequence period:
  — Only during attack / for a certain period of time
Routing Threats Consequences (1)

**Network congestion**: more traffic is routed through a specific part of the network than would usually be.

“**Blackhole**”: packets go into a certain router/region and “disappear”

**Looping**: traffic is forwarded along a route that loops (this causes both traffic to disappear and congestion)

**Partitioning**: some portion of the network believes that it is partitioned from the rest of the network when in fact it is not

**Frequent route changes**: resulting in unnecessary routing processing and message exchanges as well as large variations in forwarding delay

**Instability of the routing protocol**: convergence towards a global forwarding state is not achieved

**Routing overload**: routing protocol messages become a significant part of the overall transported traffic the network carries
Routing Threats Consequences (1)

Network congestion

“Blackhole”:

Looping:

Partitioning:

Frequent route changes:

Instability of the routing protocol:

Routing overload
Routing Threats Consequences (2)

Consequences regarding a specific target host / network:

— **Delay**: traffic from / to a target host / network is routed along routes that are inferior to the route the traffic would otherwise take

— **Cut**: some part of the network believes that there is no route to the target host / network when, in fact, there is

— **Starvation**: the traffic destined for the target host / network is routed to a part of the network that cannot deliver it

— **Eavesdropping**: traffic is routed through some router or network that would normally not “see” this traffic, so that an attacker can eavesdrop on the traffic or at least monitor the traffic pattern

— **Controlled delivery**: traffic is routed through a router / network so that an attacker can selectively delay, delete or modify packets destined to a target host / network
Routing Threats Consequences (2)

Consequences regarding a specific target host / network:

- **Delay**: traffic from / to a target host / network is routed along routes that are inferior to the route the traffic would otherwise take.
- **Cut**: some part of the network believes that there is no route to the target host / network when, in fact, there is.
- **Starvation**: the traffic destined for the target host / network is routed to a part of the network that cannot deliver it.
- **Eavesdropping**: traffic is routed through some router or network that would normally not “see” this traffic, so that an attacker can eavesdrop on the traffic or at least monitor the traffic pattern.
- **Controlled delivery**: traffic is routed through a router / network so that an attacker can selectively delay, delete or modify packets destined to a target host / network.
Generally Identifiable Routing Threats (1)

**Disclosing routing information:**
- Deliberate exposure of routing information: e.g., by a subverted router in order to disclose routing information
- Eavesdropping on routing exchanges: different attacking technique, also leading to disclosure of routing information
- Traffic analysis: by eavesdropping on forwarded data traffic, an attacker can gain insight about routing information

**Masquerade:**
- An entity claims the identity of a router (sometimes also called spoofing)
- Masquerade is usually performed in order to realize further attacks

**Interference:**
- An attacker inhibits the exchange of routing information between routers, e.g. by delaying or deleting routing messages or receipts, breaking synchronization, etc.
- The consequence is usually (partial) disruption of routing operations
Generally Identifiable Routing Threats (2)

Falsification of routing information:
— Either by an originator (forging) or a forwarder (modification)

Overclaiming:
— Announcing better routes / link capacity than available
— Goals can be to attract traffic to a certain area in order to control the traffic or to mislead the traffic so that it will not be delivered at all or with higher delay
— Consequences for the network are potential overload of single routers, increase of overall traffic load

Underclaiming:
— Announcing inferior routes / link capacities than actually exist
— Potential goals are to keep traffic out of certain areas of the network, e.g. in order to avoid forwarding of traffic at certain routers or to increase attractiveness of alternative routes
— Potential consequences are that certain destinations become unreachable, and the overall traffic load in the network increases (because packets take inferior routes)
Generally Identifiable Routing Threats (3)

**Resource exhaustion:**
- E.g. by an attacker that announces frequent changes in his routing information, or triggers a router to create an excessive amount of state information which can not be handled by other routers
- Sometimes also referred to as overload
- Goal is degradation / disruption of routing protocol operation

**Resource destruction:**
- Link destruction: either physically (“cutting”) or by strong interference
- Node destruction: e.g., physically or logically by exploiting weaknesses in the router software (OS, routing software)
- Depending on the network topology, the consequences can be either of local or global scope (single network / part of network unreachable or network partitioning)
Countermeasures: IP Fast Reroute

Link or node failures result in period of disruption to the delivery of traffic

IP Fast Reroute as restoration mechanism on network layer until network and its (Intra-AS) routing finally re-converges again

• Local backup computation without need of informing neighbors about failure

Variations of IP Fast Reroute mechanisms

• Equal Cost Multipath (ECMP)
• Loop-free Alternates
• U-Turn Alternates
• Tunnels
• Not-via Addresses
IP Fast Reroute - ECMP

Failover to detour shortest paths, so we need more paths...

Equal Cost Multi-Path (ECMP)

- Routers can reach destination by multiple preferably link-disjoint paths of same cost
- Alternate paths can be pre-computed and used in case of failure

\[
\text{cost}(r_i, d) = \text{cost}(r_j, d), \ i \neq j
\]
IP Fast Reroute – Loop-free Alternates (LFA)

Using pre-computed alternate next hop $a$ in event of link failure that disrupts primary next hop $p$

$$cost(a, d) < linkcost(a, s) + cost(s, d), \quad cost(a, d) < cost(s, d)$$

While choosing loop-free alternates, micro loops need to be prevented:

In case of failure, traffic flow from source $s$ to destination $d$ is not disrupted

Network converges in background

Failure of link $(r_0, r_2)$

- Primary next hop $p = r_2$ of node $r_0$ not reachable
- Rerouting at $s = r_0$ by using $r_1$ as LFA

Failure of primary next hop $p = r_2$ of node $r_0$

- At $s = r_1$ rerouting via $r_0$ and via $r_3$ possible
- Rerouting via $r_0$ prevented as $cost(r_2, d) < cost(r_0, d)$
IP Fast Reroute – U-Turn Alternates

LFA is topology dependent, thus in certain scenarios no LFAs exist.

U-Turn alternate: use neighbor a whose primary next hop to d is again s and that itself has loop free node protecting alternate that does not go through s.

U-Turn selection criteria:

- \( \text{cost}(a, d) \geq \text{linkcost}(a, s) + \text{cost}(s, d) \)
- s must always be primary next hop neighbor on all shortest paths from a to d that traverse s.
- Node a has a loop free alternate.

Identifying U-Turn traffic:

- Implicit identification as traffic would be usually forwarded via neighbor.
- Explicit identification via packet marking.

Example: Failure of link \((r_0, r_2)\) results in \(s = r_0\) using \(r_1\) as U-Turn alternate.
IP Fast Reroute – Tunnels

When router $s$ detects adjacent failure it uses pre-computed set of repair paths to bypass failed neighbor $v$ or failed link $e$

Tunnel is used to carry traffic to a router (tunnel endpoint) at which loop free alternate paths exist via normal forwarding

- Packets are encapsulated by $s$ and routed towards tunnel endpoint
- Tunnel endpoint decapsulated packets and forwards them according to shortest path table depending on final destination

Repair paths

- Must be created for all neighbors of $v$ plus for $v$ itself to provision for link failures
- Micro loop prevention necessary, e.g., tunnel endpoint on shortest path to $d$
IP Fast Reroute – Not-Via Addresses (1)

Not-Via Addresses are special addresses assigned to each interface.

Once failure is detected, router needs to get packet to destination not via failure.

Tunnels traffic towards the Not-via address of the protected component.

Packets addressed to a Not-via address must be delivered to router advertising address, not via component with which address is associated.

Mechanism requires participation of intermediate routers on repair path:

- Routers must be able to tell the link which they must avoid traversing from the semantics of the Not-via address.
- Every router in repair path routes tunneled traffic using shortest paths obtained by running Dijkstra on graph where protected link is excluded.
IP Fast Reroute – Not-Via Addresses (2)

Example

• Node S routes traffic to D through B and via P
• When P has failed, S tunnels traffic towards Not-via address Bp of protected component, which is interpreted as shortest path from S to B not going via P

Drawbacks

• Each router needs pre-computed backup routes
• Each router has possibility of being in any shortest path of an initiated repair
• N-1 Dijkstra calculations required for each of the N routers in the topology
So far (within AS), so good...
The Growth of The Net, Users...
Growth: Devices, Worldwide

http://www.zakon.org/robert/internet/timeline/
http://www.isc.org/solutions/survey
Hierarchical Routing

Usual routing lectures are an idealization:
- All routers are assumed to be identical
- Network is assumed to be “flat”
- ==> Dijkstra.
  ... Real world, however, looks different

Scale (>1 billion destinations!):
- Can’t store all destinations in routing tables
- Routing table exchange would overload links

Administrative autonomy:
- Internet = network of networks
- Each network admin may want to control routing in its own network

Routing on the Internet

The Global Internet consists of Autonomous Systems (AS) interconnected with each other:

- Stub AS: small corporation (only one link to the Internet)
- Multihomed AS: large corporation (multiple links, but no transit)
- Transit AS: provider

On the Internet today we see many autonomous systems (~64454)

- Have different sizes
- Exchange services with each other as equals or as provider/customer
- Have different relations to each other

Every AS has a unique number

Every AS must know a route to every network
Routing on the Internet

The Global Internet consists of Autonomous Systems (AS) interconnected with each other:

- **Stub AS**: small corporation (only one link to the Internet)
- **Multihomed AS**: large corporation (multiple links, but no transit)
- **Transit AS**: provider

On the Internet today we see many autonomous systems (>64454):

- Have different sizes
- Exchange services with each other as equals or as provider/customer
- Have different relations to each other

Every AS has a unique number

Every AS must know a route to every network