Securing Distance-Vector Routing Protocols

ISOC Symposium on Network and Distributed System Security '97

Tuesday, February 11, 1997

Bradley R. Smith
Computer Science Dept.
University of California
Santa Cruz, CA 95064
brad@cs.ucsc.edu

Shree Murthy
Sun Microsystems Computer Corp.
2550 Garcia Avenue
Mountain View, CA 94043
shree@eng.sun.com

J.J. Garcia-Luna-Aceves
Computer Engineering Dept.
University of California
Santa Cruz, CA 95064
jj@ce.ucsc.edu

[0]This work was supported in part by the Defense Advanced Research Projects Agency (DARPA) under Grant F19628-96-C-0038.

Distance-Vector Routing

- Neighboring routers exchange *routing messages* composed of one or more *routing updates*.
- Routing updates contain, at a minimum, a destination and the distance to the destination.
- A router knows the length of the shortest path from each neighbor to every destination.
- A router computes the shortest path to each destination, sending routing messages to its neighbors as needed.

Vulnerabilities and Threats

- Routing updates can be fabricated, modified, replayed, deleted, and snooped.

- Examples:
  - Unauthorized nodes can simply participate in the routing protocol dialog (i.e. no access control mechanisms are defined for the protocol).
  - Nodes can masquerade as an authorized router using source routing attacks or TCP session hijacking attacks.
  - Links can be subverted by an intruder in a manner allowing the manipulation of routing messages.
  - Subverted routers can be made to run modified software, or use a modified configuration.

Vulnerabilities and Threats (cont.)

- The threats posed by these vulnerabilities include:
  - Black hole routes $\Rightarrow$ denial of service.
  - Reconfigure logical topology $\Rightarrow$ disclosure of data traffic and inaccurate accounting of usage.
  - Routing traffic snooping $\Rightarrow$ disclosure of path information.

Assumptions

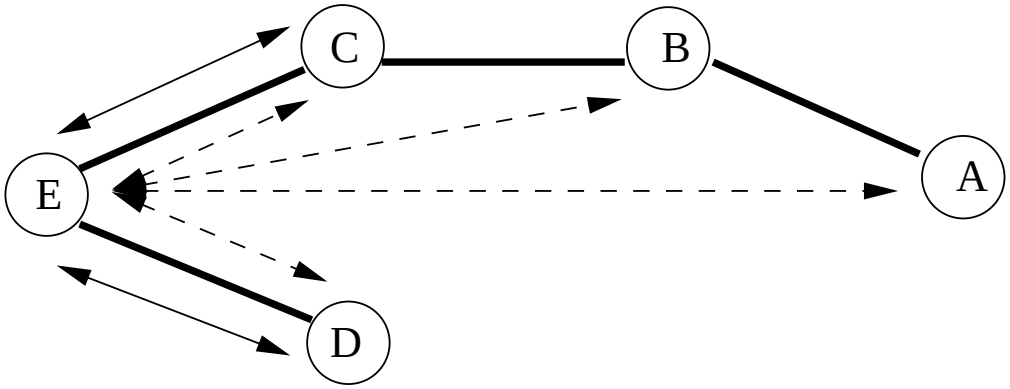
- Intruders have the capabilities described previously.
- Information received from a router can only be trusted regarding links incident on that router.
- Each router is assigned a public-key pair.
- Key distribution mechanisms are available to distribute public-keys given an IP address of a host.

Countermeasures

Message Protection: Protect the transmission of routing messages between neighbors.

Update Protection: Protect the transmission of routing updates between an originating router and a dynamically determined set of remote routers.

Classes of Information



Neighbor-to-neighbor, routing messages.

Dynamic multicast, routing updates.

Message Protection

- *Message sequence number.*
- *Message digital signature.*
- Protect messages from fabrication, modification, deletion, or replay by "outsiders" (masquerading routers, unauthorized routers, and subverted links).
- Addressed by currently proposed link-oriented, neighbor-to-neighbor countermeasures such as the use of the IP security extensions.

Update Protection

Update digital signature and originating router I.D.

- Protects all fields of a routing update, except the distance field, from fabrication or modification by subverted routers.
- Computed over all fields of the routing update (including those defined below) except the distance field.
- Originating router I.D. needed to verify digital signature.

Update sequence information.

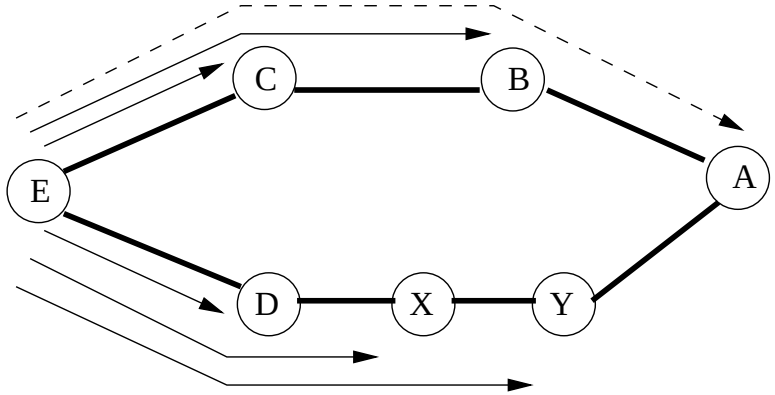
- Protect against the replay of routing updates by subverted routers.
- Timestamp $\Rightarrow$ shorter lifetime, simpler administration.
- Sequence number $\Rightarrow$ longer lifetime, more complex administration.

Update Protection (cont.)

Predecessor network.

- Indirectly protects the distance field from fabrication or modification by a subverted router via mis-representation of downstream connectivity.
- E.g. protects against a node advertising a 2 hop route to a destination that is 10 hops downstream.
- The predecessor network is the second-to-last network traversed by packets on their way to the given destination.
- Given the predecessor network for all intermediate hops to a destination, the path to the destination can be reconstructed.

Update Protection Summary



Dest	<Pred,SN>$_{Dest}$	Dist
D	< E, ... >$_D$	1
C	< E, ... >$_C$	1
B	< C, ... >$_B$	2
X	< D, ... >$_X$	2
Y	< X, ... >$_Y$	3

Information at E before A is added.

Dest	<Pred,SN>$_{Dest}$	Dist
D	< E, ... >$_D$	1
C	< E, ... >$_C$	1
B	< C, ... >$_B$	2
X	< D, ... >$_X$	2
Y	< X, ... >$_Y$	3
A	< B, ... >$_A$	3

Information at E after A is added.

D can no longer advertise a 1 hop route to A!

Countermeasure Effectiveness

Message protection countermeasures:

- protect routing updates from fabrication, modification, deletion, and replay by unauthorized routers, masquerading routers, and subverted links.

Update digital signature:

- protects all fields of a routing update, except the distance field, from fabrication or modification by subverted routers.

Update sequence number:

- protects all fields of a routing update, except the distance field, from replay by subverted routers.

Predecessor:

- protects the distance field from fabrication or modification by a subverted router.

Countermeasure Effectiveness

- Remaining vulnerabilities.

  Subverted router can:

  – fabricate information re: links incident on it,

  – delete routing updates,

  Any node can:

  – snoop routing information.

Cost of Countermeasures

Per Message:

- Space for 128bit digital signature and 32bit sequence number.
- Time to compute and validate digital signature.

Per Update:

- Space for 128bit digital signature, 32bit sequence number, 64bit predecessor address and mask, and 32bit originating router address.
- Time to compute digital signature (once per predecessor per update), and verify once per router which selects a path which uses the link.

Per Destination:

- Time to perform path-traversal for each change in route to a given destination.

Conclusions

Protection from outsiders:

- Reasonably straightforward.
- Requires sequence number and digital signature per routing message.

Protection from subverted routers:

- Can be done in constant space (i.e. linear w.r.t. number of destinations).
- Requires sequence information, predecessor information, and digital signature per routing update.
- Time and space costs are high, but not as bad as previously thought.