

Comparison of Schemes for Security of Routing Protocols

William M. Banick III

Introduction:

One of the functions of routing protocols is to dynamically configure the packet forwarding function in Internet configurations to provide for the continued delivery of transmitted packets in spite of any changes to the underlying network topology. These types of changes typically occur due the introduction, failure and repair of network links and routing nodes, which these routing protocols have been, designed to accommodate. Current routing protocols contain few, if any, mechanisms to provide for the security of their operation. For example, Border Gateway Protocol (BGP) security mechanisms protect the transmission of routed message across local networks; however BGP does not provide integrity or authentication of the routing information itself as it traverse the nodes and links that make up the internet. This paper analyzes the security requirements of routing protocols, identifies vulnerabilities, and looks at current and proposed mechanisms to counter these vulnerabilities.

Project Specifications:

1. Protocols to be compared:
 - Border Gateway Protocol (BGP).
 - RIPv2
2. Comparison of protocols based on the following factors:
 - Security (Confidentiality, Integrity and Authentication).
 - Performance.
 - Flexibility and scalability.
 - Interoperability.
 - Cost.
3. Questions to be answered:
 - What are the weaknesses in the protocols security that could be exploited by and intruder?
 - What are the current security mechanisms in place now for routing protocols?
 - How could an intruder gain access to data that the intruder is not authorized to receive?
 - How could an authorized entity receive false data?
 - How could an intruder or security violation disrupt the correct operation of the network routing functions?
 - How could an intruder or other unauthorized person gain control of the network routing functions?
 - Are there any inefficiency introduced by securing routing protocols?
 - How do current routing security protections compare against any new extensions that are available?
 - Do the security mechanisms and any new extensions protect against external attacks only?

Comparison of Schemes for Security of Routing Protocols

William M. Banick III

4. Procedure for verifying the results of the research investigation:
 - a. Research and report will be based on information gathered from published technical material including vendor white papers, books and other research articles.
5. Tentative Table of Contents:
 - a. Purpose: Explains the scope of the research and the objectives of the research.
 - b. Introduction to internet routing protocols
 - c. Key Internet routing protocols and how they work.
 - d. Current security mechanisms provided by the network routing protocols.
 - e. Current security vulnerabilities and threats to network routing information.
 - f. Proposed security enhancements to deal with the vulnerabilities.
 - g. Conclusion.
 - h. References.
6. Tentative Time Schedule:
 - ❑ October 4, 2003: Revise and submit final project specification
 - ❑ October 15, 2003: Submit first progress report. This will cover purpose, introduction and the description of the routing protocols to be analyzed.
 - ❑ October 29, 2003: Submit second progress report. This will cover the current security mechanisms, threats, how current security mechanisms protect against the threats and what the weaknesses are.
 - ❑ November 12, 2003: Submit the third progress report. This will cover the proposed security enhancements and conclusion.
 - ❑ December 3, 2003: Submit the final progress report with draft version of final view graph presentation.
 - ❑ December 6, 2003 Project report submitted.
 - ❑ December 9, 2003 Reviews of project report.
 - ❑ December 12, 2003: Final oral presentation and final written report.
7. Possible areas where the specification can change:
 - ❑ Analysis of current routing protocol security mechanisms.
8. List of references:
 - ❑ R. Atkinson Security Architectures for the Internet Protocol. RFC 1825, Aug 1995.
 - ❑ D. Bertsekas. *Data Networks*. Prentice Hall, 2nd edition, 1992.
 - ❑ B. Kumar. Integration of Security in Network Routing Protocols. *ACM IGAC Review*, 11(2):18-25, Spring 1993.

Comparison of Schemes for Security of Routing Protocols

William M. Banick III

- ❑ S.L. Murphy. Digital Signature Protection of the OSPF Routing Protocol. *Proceedings: Symposium on Network and Distributed System Security*, 1996.
- ❑ L.Lamport. The Byzantine Generals Problem. IEEE Transactions on Programming Languages and Application Systems, 4(3): 382-401, July 1982.
- ❑ Y.Rekhter. A Border Gateway Protocol 4 (BGP-4). RFC 1771, Mar. 1995.
- ❑ S. Murphy and M. Badger and B. Wellington, "OSPF with Digital Signatures," RFC 2154.
- ❑ B. Smith and S. Murthy and J.J. Garcia-Luna-Aceves, "Securing the Border Gateway Routing Protocols," *Global Internet '96*, London, Nov. 1996.
- ❑ C.Cheng. A Loop-Free Extended Bellman-Ford Routing Protocol without Bouncing Effect. *Computer Communications Review*, 19(4): 224-336, 1989.
- ❑ V.L. Voydock. Security Mechanisms in High Level Network Protocols. *ACM Computing Surveys*, 15(2): 135-171, June 1983.
- ❑ B.Kumar. Integrating Security in Inter-Domain Routing Protocols. *ACM Computer Communications Review*, pages 36-51, 1993.