Computer Networks 79 (2015) 68–90

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Router authentication, key management, and adjacency management for securing inter-router control messages

Revathi Bangalore Somanatha, J. William Atwood *

Department of Computer Science and Software Engineering, Concordia University, 1455 De Maisonneuve Blvd. West, Montréal, Québec H3G 1M8, Canada

ARTICLE INFO

Article history:
Received 8 May 2014
Received in revised form 3 December 2014
Accepted 17 December 2014
Available online 7 January 2015

Keywords:
Security
Routing
Network management
Authentication
Key management
Adjacency management

ABSTRACT

To build secure network-based systems, it is important to ensure the authenticity and integrity of the inter-router control message exchanges. Authenticating neighbors and ensuring the legitimacy of the neighbor relationships is essential. Current manual keying methods used to secure router control messages are error prone, not scalable, and result in keys being changed infrequently (or not at all) due to lack of authorized personnel. We propose an automated key management system to automatically generate, distribute and update keys for a collection of 'keying groups', each of which is the subset of routers sharing the same key. The proposed protocol for key management ensures security in the form of authentication, integrity, confidentiality, protection against replay attacks, and robustness across reboots. It has been designed to handle a wide variety of keying groups. In addition, it makes provision for adjacency management. In this paper, we describe the threat model and security requirements for the key management system. Further, we explain in detail a formal validation that we have carried out in order to verify the security of the system. Thereby we clearly show how our design meets the requirements specified.

1. Introduction

When a client logs into her bank through online banking, information is transferred from the client to the bank (and back) through the Internet. The security of the end-to-end exchange is visible to the client, if she chooses to notice the `https:` prefix in the bank's web address. However, the fact that the packets of the end-to-end exchange will traverse several routers on the Internet is invisible to the client.

Individual network segments are connected together through routers to form the global Internet. A router determines the "best path" through the Internet between two end systems by periodically exchanging *routing updates* with its neighbors. These exchanges constitute a *routing protocol*. If one or more of the (apparent) neighbors is an intruder, then the security of the end-to-end exchange can be compromised. The ability to compromise the security exists even if the `https:` prefix is present. Therefore, it is just as important to ensure the legitimacy of the intermediate routers on the path as it is to ensure the legitimacy of the client and the bank. This implies that the routing protocol exchanges must also be secured.

Methods for ensuring router-to-router security have been written into the specifications of routing protocols for many years. However, the authors of [1] note that "almost all [those who responded] report using one manually distributed key throughout the entire network. These same operators report that the single key has not been

* Corresponding author. Tel.: +1 514 848 2424x3046; fax: +1 514 848 2830.
E-mail addresses: revathi.bs@gmail.com (R. Bangalore Somanatha), william.atwood@concordia.ca (J.W. Atwood).
URL: http://users.encs.concordia.ca/~bill (J.W. Atwood).

http://dx.doi.org/10.1016/j.comnet.2014.12.015
1389-1286/

changed since it was originally installed, sometimes five or more years ago." This leaves ample opportunity for the keys to be compromised. This could lead to an intruder router pretending to be a legitimate one and capturing confidential data.

In March 2006, the Internet Architecture Board (IAB) held a workshop on the topic "Unwanted Internet Traffic". The report from that workshop is documented in [2]. Section 8.1 of that document states, "A simple risk analysis would suggest that an ideal attack target of minimal cost but maximal disruption is the core routing infrastructure". Section 8.2 calls for "[t]ightening the security of the core routing infrastructure".

One approach to achieving improved security is to automate the process of updating the security parameters. This will reduce the number of network management personnel needed and would potentially improve security for all users of the Internet. This leads us to the following requirements:

- Ensuring the authenticity and integrity of the routing protocol messages.
- Ensuring the legitimacy of the neighboring routers, by making sure that they are part of the "permitted adjacency" as explained below.
- Automation of the entire process of key and adjacency management.

The notion of "permitted adjacency" can be re-stated as providing answers to the following questions:

- Are you a legitimate member of my group? This is the question of *authentication*.
- Are you permitted to connect to me for the purposes of this routing protocol? This is the question of *authorization*.

Atwood [3] has presented motivation for router security and a description of an architecture for an authentication and key management system. The Keying and Authentication for Routing Protocols (KARP) working group of the Internet Engineering Task Force (IETF) has developed a Design document [4] and a Threats and Requirements document [1] to provide guidance for the work of improving routing protocol security.

This paper extends Atwood's [3] design, and proposes a methodology for ensuring the authentication and authorization of a peer router, and conveying the necessary policy information to do so. The methodology includes a set of interactions that meet most of the security and operational requirements specified in [4,1]. The protocols implied by this set of interactions have been formally validated for their security properties.

Section 2 explores the previous work on secure routing. Section 3 introduces our idea of Key Scopes. Section 4 outlines the specific problem that we are addressing. In Section 5, we compile the set of requirements to be satisfied by a secure, automated key management system. Following that, in Sections 6 and 7, a design is proposed that satisfies all of the compiled requirements. Sections 8–10 show the formal validation that proves the strength of our proposal. Section 11 concludes the paper.

2. Previous work

In this section, we shall see the background pertaining to the key management problem that we are trying to solve. We shall see the works in existence and the area where there is need for additional work. We shall also see some concepts and terminology used in the paper.

2.1. Routing protocols

Routers in the Internet exchange among themselves details of network reachability and path costs so that they can forward packets along the path associated with the least cost. We adopt the definition of an Autonomous System (AS) from [5]: an AS is a set of routers under a single administration and having a single routing policy. Routing Protocols can be classified as Interior Gateway Protocols (IGPs) (within an AS) or Exterior Gateway Protocols (EGPs) (among ASes). Routing Protocols can also use unicast or multicast transmission to exchange their route updates or other pertinent information.

We define the concept of an Administrative Domain (AD). For a particular routing protocol, the network as a whole is divided into one or more ADs. An AD is a set of routers with a common policy. An AD might encompass a collection of routers spanning two or more ASes, or all of the routers inside a particular AS, or only a small subset of the routers inside an AS, for instance.

A very important requirement of routing protocols and the routing updates exchanged is security, which we shall discuss now.

2.2. Security aspects

Routers in the Internet continually exchange control messages. An intruder could eavesdrop on these messages and modify them so as to have all data sent towards himself. Depending on the severity of the attack, the results could even be disastrous. This implies that the control message exchanges among routers have to be made secure.

There are two aspects to the security. The first is that the distributed information is from an authenticated source, and has not been altered. This is the concern of the KARP [6] working group. The second is ensuring the validity of the *contents* of the exchanged material. This is the concern of the Secure Inter-Domain Routing (SIDR) [7] working group.

In this paper, our focus is on the management of the keying material for securing router control packets within an AD. Therefore the work of the KARP working group is most relevant to us.

As mentioned, KARP has produced two documents that set the basis for the requirements and design of protocols that intend to address the security of routing protocols. These documents are the Design document [4] and the Threats and Requirements document [1]. Both of these