

Secure Link State Routing Protocol: A Framework

Dijiang Huang
{dhuang@conrel.sice.umkc.edu}
University of Missouri – Kansas City

Abstract— There are several security threats that are not addressed or partially addressed in current link state routing protocol. We propose a new framework for secure link state routing protocol based on two cryptographic countermeasures: information-level data origin authentication and information-level confidentiality. This new framework constructs multiple *virtual trust routing domains* (VTRD) to constrain certain very “hard” security threats. Our robustness analysis and simulations show that our framework has practical merit.

Index Terms— Authentication, Confidentiality, Group communication, Link state routing protocol.

I. MOTIVATION

There are various types of security threats a network routing protocol such as the link-state protocol can face. The existing approaches address some of these threats by securing the link state routing protocol with a certain level of authentication of the routing information packets. Several proposals have been done to enhance security in network routing protocol, but do not capture many other types of vulnerability [4].

A recent survey by Papadimitratos and Hass highlights the fact that the countermeasures proposed so far has not eradicated the vulnerability of the routing infrastructure [8]. We analyze the possible threats to a link state routing protocol and corresponding cryptographic countermeasures to guard against them. The technical details is specified in our work [4]. We classify network routing threats into five categories based on cryptographic countermeasures and the efficiency of using them:

- 1) Using *packet-level authentication* (PA)¹. Such as outsider² attacks: falsification (substitution and insertion), masquerade and overload.
- 2) Using *information-level authentication* (IA)³. Such as insider⁴ attacks: falsification (substitution, spoofing) and repudiation (false denial of origin).
- 3) Using *information-level confidentiality* (IC)⁵. Such as outsider attacks: wiretapping; insider attacks: undeliberate exposure.

¹Authenticating an entire routing or IP packet.

²The illegitimate devices that lie outside the link state routing security perimeter. The security perimeter defines who are eligible network routing participants.

³Authenticating a piece of routing information (usually an LSA). When end-to-end IA is provided, it is called information-level data origin authentication.

⁴The legitimate devices that lie inside the link state routing security perimeter.

⁵The confidentiality is provided for routing information carried by a routing packet. Using IC, a link metric can be encrypted/decrypted by a certain group of routers.

- 4) Using *information-level confidentiality* (IC) to limit both outsider attacks: interference and insider attacks: Overload and deliberate exposure.
- 5) Cryptographic countermeasures can not provide protection. Such as insider insertion and stop forwarding.

We suggest that routing protocol itself should provide immunity to prevent attacks from taking place in an inexpensive way. Based on two cryptographic countermeasures, IA and IC, we propose a new framework for secure link state routing protocol. The framework can be of benefit for:

- Preventing attacks that are listed from 1) to 3).
- Confining attacks that are listed as 4) within a certain range. We call this range is formed by *virtual trust routing domain* (VTRD).
- Providing IA and IC that can consolidate evidence for *intrusion detection system* (IDS) to locate attack source for some “hard” attacks.
- Providing imbedded security base (from control plane point of view) that network services can rely on.

II. OUR APPROACH

The new secure framework is composed using multiple VTRDs. Within a VTRD, a subset of routers construct their own routing region. Multiple VTRDs can exist within the same link state administrative domain. They can overlap or totally independent. A router can only see the routing traffic pattern within its own VTRD. The formation of VTRD can be managed by *network resource management* (NRM) system and using two cryptographic techniques: IA and IC. These two cryptographic techniques are based on symmetric key schemes, such as HMAC [6] and AES [1], which target to reduce computation overhead compared to asymmetric key scheme. To provide IA, IC and also to build multiple VTRDs, a versatile group keying scheme is required. Thus, we propose a novel *secure group communication keying scheme* (SGCKS) [3], which is based on hash function. Using SGCKS, a group of routers can construct any sub-group communication within the group without collusion problem.

Based on SGCKS, we propose *double authentication* (DA) scheme [5]. DA is an authentication scheme that authenticates each *link state advertisement* (LSA) twice, with two different sub-group keys. One sub-group key is used by a router and its communication adjacency and another sub-group key is used by the sub-group containing every other group member except its communication adjacency. Thus, an authentication chain can be built along the propagation path of a LSA. We have found that DA scheme to be able to prevent insider attacks (a) when there

is only one subverted router, and (b) multiple non-colluding subverted routers, and help to detect (c) multiple colluding subverted routers, but they can not partition the network.

Another application of SGCKS is IC. IC means the propagated routing information is not totally understandable for a router within the link state routing domain. Thus, the trust relation is not only between two communication neighbors, but also a sub-group of routers within the link state routing domain. These sub-group of routers form a VTRD. The information availability is based on sub-group key (served as *key-encrypting key* – KEK) used for particular VTRD. IC is provided during the procedures of routing data transmission and validation; note that providing IC does not change the structure of link state database and routing table. Since the confidentiality is provided based on VTRD, routers may have different view of overall network, which is determined by how many VTRDs a router belongs to (the technical details is specified in [4]). Note that the NRM allocates the network resource for each VTRD, which is a separated management system apart from network routing within the network control plane.

III. IMPLEMENTATION ISSUES

Based on our proposed framework, the implementation issues will be classified into three aspects. We describe them as follows:

First, “What are the modifications we need to do for the exist routing protocols, for example, OSPF?” One of our design goals is to minimize the modifications. OSPF itself has the extensibility for introducing new types of LSA [2]. The DA and IC can be carried out through this extension. Only the examination of VTRD and corresponding sub-group key are added into processing state machine of OSPF packet transmission and reception. All other functions and structures of OSPF remain the same.

Second, “Could a current generation router handle the add-in complexity of cryptographic operations?” Note that using SGCKS will increase the memory requirement of a router. Furthermore, signing/verifying and encrypting/decrypting operations will increase the CPU processing usage time. Based on the robustness analysis and simulations presented in [4], we show that memory overhead is reasonable for practical use. In order to reduce the computation overhead, we suggest using symmetric key scheme instead of asymmetric key scheme. For current size of link state routing domain and the number of LSAs, the CPU usage time will not exceed the CPU usage time proposed by shortest path algorithm, which is considered to be the CPU computation bottleneck of a router.

Third, “Would the new framework change the operational process of network routing and data packets forwarding?” Although multiple VTRDs exist within a link state routing domain, the fundamental routing process and the overall routing administration domain remain unchanged. Each router maintains a single link state database and the link capacity is accumulated view for all VTRDs. NRM will take the responsibility to forward the data traffic based on the routing table. Multiple VTRDs require that the network has link bandwidth management capability (note that the current best-effort network may not have this ability).

Our research plan includes two parts, namely, road map and open issues. We discuss each of them accordingly.

A. Road Map

We propose a three-stage research plan for secure link state routing protocol. The first stage is to collect security issues regarding to link state routing protocol and other corresponding network supporting systems. In this stage, the fundamental link state routing vulnerability analysis, threats categorizations and possible countermeasures are investigated.

In the second stage, based on the investigation of first stage, a possible secure link state framework is proposed and corresponding security analysis, simulations are processed to validate the proposal.

Finally, in the third stage, we investigate the implementation issues to make our approach practical.

Currently, we are in the middle of the second and third stages.

B. Open Issues

We have proposed a secure framework for link state routing protocol. The original work is targeted to provide protections for link state routing protocol and routing information. But, the new framework will also come up with many other add-in issues related to rest of exist network components. Here, we list two obvious ones.

- Network stability issue: based on our new proposed framework, each router may have different view of network topology and traffic allocation pattern. Would this will cause instability of network traffic forwarding?
- Network service supporting issue: multiple VTRD is originally designed to limit threats within a certain range (or level). The network resource is allocated through NRM in a static centralized control fashion. How to make multiple VTRDs support multiple network services distributively and/or dynamically?

REFERENCES

- [1] AES Algorithm (Rijndael) Information, <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/>.
- [2] R. Coltun, “The OSPF Opaque LSA Option”, RFC 2370, July 1998.
- [3] D. Huang and D. Medhi, “A Group Keying Scheme to Support “Any to Any” Secure Subgroup Communication”, Submitted for publication. Available at <http://conrel.sice.umkc.edu/HRP/reports/huang02-fsgc.pdf>
- [4] D. Huang, A. Sinha and D. Medhi, “On a Framework for Secure Link State Routing Protocol”, submitted for publication. Available at http://conrel.sice.umkc.edu/HRP/reports/huang03-new_framework.pdf.
- [5] D. Huang, A. Sinha and D. Medhi, A Double Authentication Scheme To Detect Impersonation Attack In Link State Routing Protocols, Accepted for publication and presentation at IEEE International Conference on Communications (ICC 2003), Anchorage, Alaska, USA on May 11-15, 2003.
- [6] H. Krawczyk, M. Bellare and R. Canetti “HMAC: Keyed-Hashing for Message Authentication”, RFC2104, February 1997.
- [7] J. Moy, “OSPF version 2”, RFC 2328, April 1998.
- [8] P. Papadimitratos and Z. J. Haas, “Securing the Internet Routing Infrastructure,” *IEEE Communication*, October 2002.