Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

A Secure Link State Approach for Network Security

Qing Cao
University of Missouri at Kansas City

A Secure Link State Approach for Network Security

Qing Cao
University of Missouri at Kansas City
caoq@umkc.edu

ABSTRACT

The pervasive nature of today's information infrastructure coupled with recent threats for cyber terrorism makes network (i.e., internal network and Internet) infrastructure security a critical issue for both computer security practitioners and researchers. Among various network security issues, a routing attack (i.e., attacks against routing protocols or attacks using routers) is the most noticeable as it can bring down a network infrastructure without causing any physical damage to the network entities. We discuss these potential attacks and propose a new secure routing framework based on security techniques (authentication and confidentiality) for a link-state routing protocol. The proposed framework emphasizes the use of efficient cryptographic countermeasures for network survivability against security threats to link-state routing protocol. The framework relies on providing information level authentication and information level confidentiality that can be imbedded in link-state routing protocol with assistance of a key management system that uses secure group communication.

Keywords

Information Systems Security, Network security, Link-state network routing, Authentication

INTRODUCTION

The threat from computer crime and other information security breaches continues unabated, and that the financial toll is mounting. According to a recent survey of 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities by the Computer Crime and Security Institute and U.S. Federal Bureau of Investigation, 90 percent of respondents detected computer security breaches within the last twelve months and the reported financial losses from these surveyed organizations were $455 million (Power, 2002).

The pervasive nature of today's information infrastructure coupled with recent threats for cyber terrorism makes network (i.e., internal network and Internet) infrastructure security a critical issue for both computer security practitioners and researchers. However, the research in network security primarily has been focused on securing the information rather than securing the infrastructure itself (Chakrabarti and Manimaran, 2002; Papadimitratos and Haas, 2002.) The FBI survey (Power, 2002) reported that $86 million in financial losses were contributed to just network breaches (i.e., unauthorized insider access, insider net abuse, denial of service, and system penetration). As such, there is a compelling need to develop architectures, algorithms, and protocols to create a reliable network infrastructure (Chakrabarti and Manimaran, 2002; Forrest et al., 1997; Houle et al., 2001; Stinson, 1997; Viega, 2001.)

Among various network security issues, a routing attack (i.e., attacks against routing protocols or attacks using routers) is the most noticeable as it can bring down a network infrastructure without causing any physical damage to the network entities (Chakrabarti and Manimaran, 2002; Papadimitratos and Haas, 2002.) The lack of strong protection by using cryptographic techniques as part of the original routing protocol design has allowed malicious users to exploit the network in numerous ways. In recent years several standards have been created to handle a variety of routing threats in order to make the routing protocol more robust. For instance, link-state protocols such as the open shortest path first (OSPF) of transmission control protocol/Internet protocol (TCP/IP) and intermediate-system-to-intermediate-system (IS-IS) of open systems interconnect (OSI) reference model are widely used for intra-domain routing (Papadimitratos and Haas, 2002.) However, network routing still remains vulnerable in both the routing protocol itself and routing functionalities involved with sending and receiving routing data. The first security issue with the current routing frameworks is its ambiguousness of non-host based threats for link-state network routing protocol, such as the threats targeting at origination, verification, and transmission of routing data. Thus, it is possible that an attacker can wiretap on the transmission link to inject anything, and an attacker can also have the capability to "hijack" the network router and then breach the network as desired. The second security issue, which has not received much attention in network routing, is confidentiality (i.e., assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended). For example, confidentiality was not considered in OSPFv2 or has been considered as optional in OSPFv3 (Papadimitratos and Haas, 2002.) An advantage of confidentiality is that it can guard against passive attacks, such as wiretapping. The routing information can be easily intercepted on unprotected network segments in its absence. Since the fundamental communication operation of link-state routing protocol is flooding, the attacker can easily intercept all routing information just from one network segment and then use it to analyze network topology and traffic patterns in exploiting the weaknesses of the network and launch more devastating and highly efficient attacks. For example, an attacker can split the network and disable it by attacking the minimal number of nodes that partition the network.

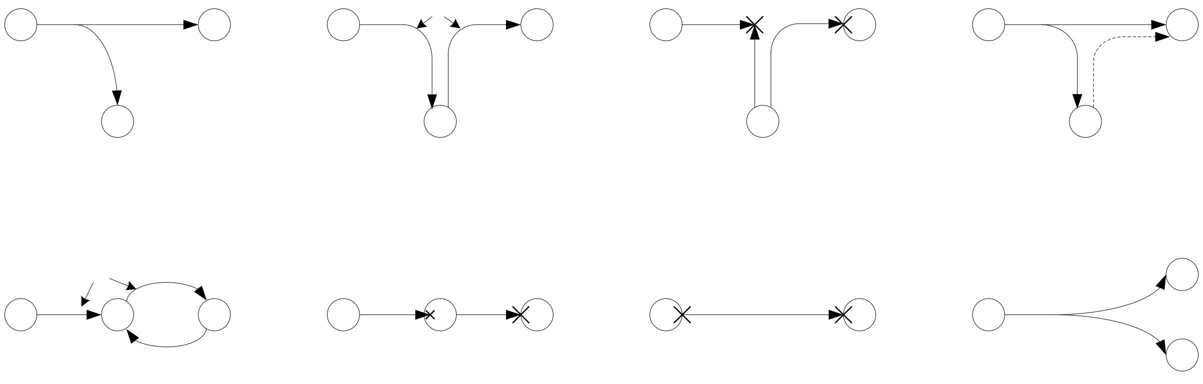
TAXONOMY OF NETWORK ROUTING THREATS

Our study outlines various types of network routing threats based on the origination, verification, and transmission of routing data. The universe of network threat is divided into two categories based on threat sources: insiders and outsiders. This classification helps to categorize corresponding preventive cryptographic countermeasures which will be discussed in the next section. The legitimate devices that lie inside the link-state routing security parameter are called *insiders*. The devices that lie outside the link-state routing security parameter are called *outsiders*. The security parameter defines a router/link's authorized role in network routing, which includes two parts: identity and functionality. For example, a valid router (or an insider) is authorized to perform routing functions, such as exchanging routing information, and associates with a unique router ID. Unfortunately the insider and outsider definitions can be confusing because of their masquerading functions. An outsider can masquerade to generate routing information just like an insider, if it has no valid identifier and is not authorized to perform routing functions. An insider can also masquerade as another authorized router and generate forged routing information, if it has a valid identifier but it is not authorized to impersonate other routers or forge other routers' routing information. To clarify this issue in our framework, our definition of *authorized* is from overall routing operational functionalities per se. For example, a router/link is authorized as part of routing domain to exchange routing information and possesses a valid identifier. By this definition we are saying an outsider is unauthorized and an insider is authorized. Figure 1 illustrates the classification of network routing threats.

Attacks by outsiders include:

(a) *Sniffing*: Monitoring and recording routing data transmitted on the communication *Insertion*: introducing malicious routing data to links among routers; see Figure 1(a).

(b) *Falsification and masquerading* comprise of three subcategories: (1) *Substitution*: altering or replacing valid routing information with false routing information; see (1) in Figure 1(b), (2) *Insertion*: introducing false routing data that serves to deceive an authorized router; see (2) in Figure 1(b), and (3) *Masquerading*: impersonating an authorized link/router; see (3) in Figure 1(b).



(c) *Obstruction* consists of two elements: (1) *Interference*: an attacker can block the transmission link by cutting off the transmission link or introduce noise into the transmission link to prevent the victims from receiving the routing information correctly; see (1) in Figure 1(c) and (2) *Overload*: an attacker can place excess dummy routing traffic that can saturate the victim's input buffer or exhaust victim's CPU capacity; see (2) in Figure 1(c).

(d)-(1) *Replay* (attack): a valid routing data transmission is maliciously or fraudulently repeated by an outsider; see (1) in Figure 1(d).

Attacks by insiders include:

(d)-(2) *Replay*: a valid routing data transmission is maliciously or fraudulently repeated by an insider; see (2) in Figure 1(d).

(e) *Falsification and masquerading*: The same as what is specified in outsiders' attacks; see (1), (2), and (3) in Figure 1(e).

(f) *Obstruction* involves two categories: (1) *Stop forwarding*: the subverted router does not forward received routing packets; see (1) in Figure 1(f) and (2) *Overload*: excessive routing information processing burden is placed on the router in order to saturate the victim's input buffer or exhaust victim's CPU capacity; see (2) in Figure 1(f).

(g) *Repudiation* contains: (1) false denial of origin: a subverted router denies the operations that it had done on the transmitted routing information; see (1) in Figure 1(g) and (2) false denial of receipt: a subverted router denies receiving the routing data; see (2) in Figure 1(g).

(h) *Exposure* contains: (1) *Undeliberate exposure*: a router unintentionally release sensitive routing data to attackers (both insiders and outsiders); see (1) in Figure 1(h) and (2) *Deliberate exposure*: a subverted router intentionally releases sensitive routing data to attackers; see (2) in Figure 1(h).

CURRENT NETWORK SECURITY MECHANISMS

The challenges posed due to the enormity and diversity of the network threats has led to several studies in the recent years that address techniques to safeguard a network. In order to properly discuss how to prevent network attacks from taking place, we must first delineate the widely used preventive cryptographic countermeasures.

Preventive cryptographic countermeasures

In Table 1 the two main preventive cryptographic countermeasures for routing protocols are *authentication* (i.e., assurance to one entity that another entity is who he/she/it claims to be) and *confidentiality*. The data origin authentication service provides verification that the identity of the original source of a received data unit is as claimed. Confidentiality ensures that no unauthorized device can decipher the routing information on its way to the destination. These two countermeasures can provide protection at either *packet level* (PA) or *information level* (IA). By PA we mean the authentication is processed for a routing update packet or an IP packet that contains the routing update as payload. IA provides protection for the routing information carried within a routing update packet. Besides PA and IA, there are another two important concepts we need to introduce; they are *hop-by-hop* (HBH) and *end-to-end* (ETE). HBH means that generation and verification of the authentication code are performed by every forwarding router. ETE means that the generation of authentication code is performed only at the source; all the forwarding routers and termination routers are part of the end system, and they only perform verification. As shown in Table 1 we also differentiate between PA and IA for confidentiality.

Methods	Level	Label	Description	Protection
Authentication (A)	Packet Level	PA_{HEH}	Packet level, hop by hop authentication	Data Origin Authenticity
		PA_{ETE}	Packet level, end to end authentication	
	Information Level	IA_{HEH}	Information level, hop by hop authentication	
		IA_{ETE}	Information level, end to end authentication	
Confidentiality (C)		C_{PA}	Confidentiality for the whole packet	Information Availability
		C_{IA}	Confidentiality for the information within the packet	

Table 1. Security mechanisms

Mapping between Preventive Cryptographic Countermeasures and Network Threats

We next outline and analyze how to use cryptographic countermeasures presented in Table 1 to guard against the threat actions illustrated in Figure 1. Table 2 shows the mapping of threats and corresponding countermeasures. The threat actions marked with √ are all outsider attacks. Using the Figure 1 labels for each type of attack, Attacks (b) can be easily guarded against by using PA_H. The dummy routing traffic due to attack (c)-(2) can be also filtered out using PA_H. Although, cryptographic-based operation can aggravate the CPU computation burden, the overload attack is usually limited within a small range where it happens. This is because the excess routing traffic cannot get through a router. This may be useful in preventing *distributed denial of service* (DDOS).

Threats		Preventive Countermeasures	Remarks
Threat actions (Attacks)	Figure 1 Label for Attack		
Substitution (OFM)	(b)-(1)	PA_{HEH}	√
Insertion (OFM)	(b)-(2)	PA_{HEH}	√
Masquerading (OFM)	(b)-(3)	PA_{HEH}	√
Overload (OO)	(c)-(2)	PA_{HEH}	√
Substitution (IFM)	(e)-(1)	IA_{ETE}	*
Masquerading (IFM)	(e)-(3)	IA_{ETE}	*
False denial of origin (R)	(g)-(1)	IA_{ETE} or IA_{HEH}	*
Wiretapping	(a)	C_{PA} or C_{IA}	**
Outsider replay	(d)-(1)	New Keys	**
Insider undeliberate exposure	(h)-(1)	C_{PA} or C_{IA}	**
Interference (OO)	(c)-(1)	C_{PA} or C_{IA}	***
Insider replay	(d)-(2)	C_{IA}	***
Overload (IO)	(f)-(2)	C_{IA}	***
False denial of receipt (R)	(g)-(2)	PA_{HEH}	***
Insider deliberate exposure	(h)-(2)	C_{IA}	***
Insertion (IFM)	(e)-(2)	n/a	¶
Stop forwarding (IO)	(f)-(1)	n/a	¶

Table 2. Network threats and corresponding countermeasures

OFM: Outsider Falsification & Masquerade; OO: Outsider Obstruction; IFM: Insider Falsification & Masquerade; IO: Insider Obstruction; R: Reputation

Attacks marked with * (i.e., (e)-(1), (e)-(2) and (g)-(1)) can be foiled by using IA_{ETE} or IA_{HEH}. Attacks marked with ** (i.e., (a), (d)-(1) and (h)-(2)) can be thwarted by using C_{PA}, C_{IA} or key management. We can use preventive cryptographic countermeasures to provide degree of protection to link-state routing from attacks marked with ***. However, effectively limiting these attacks (i.e., (c)-(1), (f)-(2) and (h)-(2)) is still a very challenging task. Unfortunately, there is no countermeasure for the threat actions marked with ¶.

The current standards for network routing protocols have not incorporated all the techniques required to make it as foolproof as possible in preventing network attacks. Moreover, current network routing lacks a framework for survivability under security threats to routing protocol (Houle et al., 2001; Moyer et al., 1999), especially dealing with certain types of attacks (i.e., ** and ***). As a result, a set of unplugged security holes remain and as such an adversary can use them to paralyze a network. Literature (Chakrabarti and Manimaran, 2002; Hauser et al., 1999; Moyer et al., 1999; Papadimitratos and Haas, 2002) strongly suggests that a new network routing framework is needed to deal with the network threats.

SECURE LINK-STATE NETWORK ROUTING FRAMEWORK

In this study, we propose a secure routing framework based on security techniques (authentication and confidentiality) for the link-state routing protocol. There are many network routing frameworks to guard against network attacks marked as √ and * in Table 2. The goals of the proposed security framework are to safeguard the network routing protocol from threats marked by ** and to limit the extent of damages that can be caused by the attack marked with ***. Figure 2 provides an overview of the framework proposed in this study. There are five components in the framework: virtual trust routing domains (VTRDs), network resource management (NRM), key management (KM), traffic management (TM), and intrusion detection system (IDS). Arrows within Figure 2 represent the communication relations among different components. The entire routing domain can be divided into multiple virtual routing domains with a hierarchical trust among them. We refer to each such domain as a *virtual trust routing domain* (VTRD). The framework does not need or imply the division of the administrative domain (i.e., of intra-domain routing). Every router that belongs to a particular VTRD will have complete routing information of its own domain, but limited information on other VTRDs, depending on the level/group it belongs to. This feature of VTRD would ensure that the damage caused by attacks marked with *** are restricted within the VTRD to which the compromised router/link belongs. The *network resource management* (NRM) plays an important role for our framework to provide survivability. It serves as a coordinating center to create or withdraw a VTRD. The *traffic management* (TM) and *intrusion detection system* (IDS) report network status and security events to the NRM. Based on the information, NRM makes the decision on creating or withdrawing a particular VTRD.

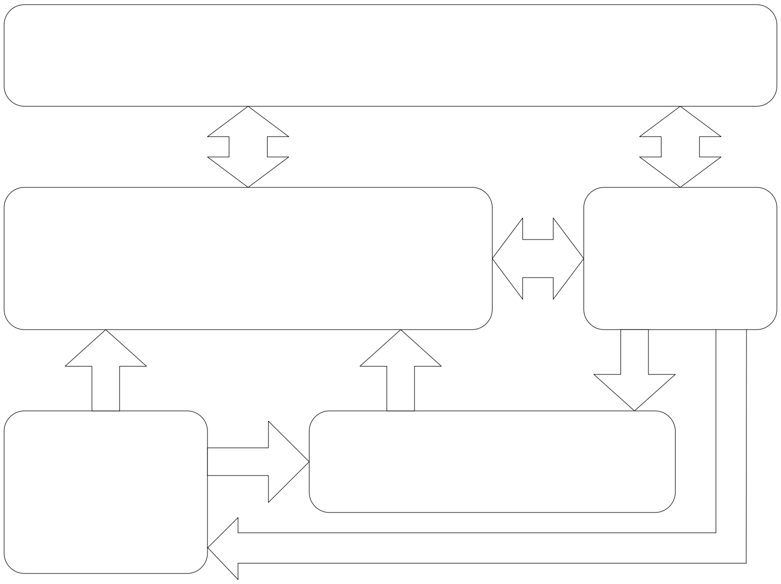


Figure 2. Network routing security framework

An efficient *key management* (KM) needs an efficient keying scheme that can reduce the management overhead. Creating VTRDs in a routing domain, providing IA and confidentiality to the routing information require an efficient symmetric keying scheme. The keying scheme would be deemed suitable for this purpose if it displays the following features:

- Due to frequent routing information exchange, the use of shared key scheme is desired in order to minimize computational overhead.
- KM needs to be flexible in order to support group/subgroup communication to reduce overhead caused by subgroup formation process.

To build VTRDs, the proposed frame ensures the independence among all VTRDs that provide strong survivability when a router is compromised. Any single router failure of a VTRD would not affect other VTRDs. (Please see appendix for how to evaluate the proposed framework.)

BENEFITS OF THE PROPOSED FRAMEWORK

An evaluation model was created as a part of this study to analyze the robustness of the proposed framework. A summary of the evaluation results of the framework have shown the following benefits:

- The framework prevents attacks marked * and **, and limits damages of attacks marked ***.
- Proposed security features are adds-on components and hence do not change operational functionalities of current link-state routing protocols.
- Most threats targeted at link-state routing can be prevented by using preventive cryptographic countermeasures.
- Routers have the ability to handle the extra processing required for the proposed framework, with some increase in memory requirement.

CONCLUSION

Network survivability has been studied extensively from the view of node and link failures. The domain of survivability goes beyond just the physical failures and one needs to address this issue when faced with security threats that can render the network logically dysfunctional without causing any physical damage. Our analysis shows that a network routing protocol (i.e., the link-state protocol) may encounter several security threats which will eventually cause network routing networks susceptible to a number of attacks. We discuss these potential attacks and proposed a new secure routing framework based on security techniques (authentication and confidentiality) for a link-state routing protocol. The proposed framework emphasizes the use of efficient cryptographic countermeasures for network survivability against security threats to link-state routing protocol. The framework relies on providing information level authentication and information level confidentiality that can be imbedded in link-state routing protocol with assistance of a key management system that uses secure group communication. We feel our study provides today's security professionals with an efficient weapon to deal with network attacks in that imbedding this framework to an existing protocol can be done without major modifications to the existing protocol, and without affecting its operational features.

REFERENCES

1. Chakrabarti, A. and Manimaran, G. (2002) Internet infrastructure security: A taxonomy, *IEEE Network*, 16, 6, 13-21.
2. Forrest, S., Hofmeyr, S., and Somayaji, A. (1997) Computer immunology, *Communications of ACM*, 40, 10, 88–96.
3. Hauser, R., Przygenda, T., and Tsudik, G. (1999) Lowering security overhead in link-state routing, *Computer Networks*, 31, 8, 885–894.
4. Houle, K. J., Weaver, G. M., Long, N, and Thomas, R. (2001) Trends in Denial of Service Attack Technology. CERT Coordination Center, 2001.
5. Moyer, M.J., Rao, J.R., and Rohatgi, P. (1999) A survey of security issues in multicast communications, *IEEE Network*, 13, 6, 12-23.
6. Papadimitratos, P. and Haas, Z.J. (2002) Securing the Internet routing infrastructure, *IEEE Communications*, 40, 10, 60-68.
7. Power, R. (2002) CSI/FBI computer crime and security survey. *Computer Security Issues & Trends*, 8, 1, 1-22.
8. Stinson, D.R. (1997) On some methods for unconditionally secure key distribution and broadcast encryption, *Designs. Codes and Cryptography*, 12, 3, 215-243.
9. Viega, J., Konho, T., and Potter, B. (2001) Trust (and mistrust) in secure applications, *Communications of ACM*, 44, 2, 31–36.

APPENDIX – EVALUATION OF SURVIVABLE NETWORK FRAMEWORK

In this section, we analyze the control plane failures and then set up the evaluation model to analyze the robustness of presented VTRD framework. Conceptually, network failures include physical network devices failure and logical network failure. Physical network devices failure include nodes failure and links failure. The corresponding damages to the network are straightforward. The device is either functional or dysfunctional. In this paper, we consider the physical network devices failure as a consequence of an attack. The possible failure size/range of physical network is one of parameter to evaluate our presented framework.

A. Logical network failure

We define the logical network failure as an attacker hacking into the system and utilizing the system resource to deploy network attacks. It is also called *Byzantine* failure which can cause more damage than just simple link or node failures. The attacker can utilize network control plane, i.e. routing, to deploy more efficient attacks to cause wide area network turbulence or intercept critical data traffic. Moreover, it is hard to locate logical network failure as compared to physical network failure, because attackers always try to hide their location and make the network suffering longer.

Based on attack consequences, we classify the network failure caused by attacks into two types:

1. *Type-I* Information based failure: the attacks target at deriving network resource allocation information.
2. *Type-II* Operation based failure: the attacks target at compromising or misleading network operation.

When an attacker hacks into a network router, we call the router as a subverted router. As a result, we assume an attacker takes over the router and usurp all the knowledge the subverted router has. To analyze *Type-I* failure, we use *P* to represent the overall information of a link state routing domain, S_{ri} represents the information known by a router *ri*. Thus, we have equation:

$$L_{ri} = S_{ri}/P \qquad (1)$$

where, L_{ri} represents the proportional information a router *ri* has, where there are n routers within the link state routing domain, i = 1,…, n and $P = (S_{ri},\ldots, S_{rn})$. We define the information survivability as Γ, which represents the proportion of safe information, i.e.

$$\Gamma = \sum_{i}^{\text{good}} \text{Lri} \qquad (2)$$

where ri is a good router. If we consider that each router has equal probability to become a subverted router, obviously, $L_{r1} = \ldots = L_{rn}$ is the condition to minimize the variance $V_k(\Gamma)$ of k subverted routers, where k < n. Accordingly, the expectation $E_{n-k}(\Gamma)$ represents the survivability of a link state routing domain with k subverted routers. The condition $L_{r1} = \ldots = L_{rn}$ specifies that the survivability is router independent. In real network, some router may get more security preference than others, such as minimum network cut routers, edge routers, etc. In this paper, to make the analysis easier, we assume all routers have same security preference. The survivability analysis based on *Type-II* failure is similar to the analysis of *Type-I* failure. Based on our proposed VTRD framework, the consequence of failure is the incidence of overall network, i.e. the proportional number routers that recognize the VTRD session key. This is based on the fact that, within a VTRD, a subvertedrouter can compromise or mislead other routers that use the same VTRD session key. Thus, for *Type-II* failure, we still can use the survivability Γ defined in the analysis of *Type-I* failure.

B. Survivability Analysis

To find the maximum survivability Γ, we need to define *P* and L_{ri} to fulfill Equations 1 and 2. The VTRD framework proposed in Section IV is based on subsets of routers within the link state routing domain, and within a VTRD all routers use a shared VTRD session key to disseminate routing information. Thus, we define *P* as the set of all possible VTRDs of a link state routing domain. We note that a VTRD is composed by a subset of routers, which is connected by communication links.

To form a virtual routing domain, a VTRD needs to provide end-to-end guarantee to support data traffic. This means that there should have at least an ingress router and an egress router. Thus, the minimal composition of a VTRD is the routers on a routing path within the link state routing domain. In our analysis the granularity of a VTRD is a routing path within the link state routing domain. We then use *P* to represent all possible routing paths within the link state routing domain. The Sri is one possible routing path that contains router *ri*. Our optimization goal is to maximize Γ, in other words, to minimize the effect of a node failure. It is equivalent to making P as big as possible as well as to make Sri as small as possible. One way to achieve this is to distribute VTRD session keys evenly and to avoid depending on some nodes heavily. Once router *ri* is compromised, it will affect all VTRDs that contains *ri*. All other VTRDs that do not contain ri will not be affected. Thus, the survivability defined in Equation 2 is also referred as usable rate under network stress.