Electronic and Computer Engineering Master
Program Faculty of Engineering
Al-Quds University

Thesis Approval

Detecting Misdirection Attack in Link-State Routing Protocols

By

Student Name: Mohammed Abed Al-majid Odeh
Reg. No: 20714130

Supervisor: Dr. Rushdi Hamamreh

Master thesis submitted and accepted. Date:--21/8/2011---

The names and signatures of the examining committee members are as follows:

1- Head of Committee Dr. Rushdi Hamamreh Signature: ----------

2- Internal Examiner Dr. Rashid Jayousi Signature: ----------

3- External Examiner Dr. Radwan Tahboub Signature: ----------

Abstract

The internet was originally designed to be trustworthy, reliable and extensible, while its infrastructure, mainly the routing mechanisms, was not constructed with security in mind. Moreover, routers are subject to malicious attacks targeting not only a single subnet or individual user, but also the overall network performance. One of the subtle attacks is that an adversary could compromise a router, leaving the control-plane (i.e. the part where routers apply the routing protocols to exchange control and update messages that discover the network topology and compute the shortest paths) operate properly in order to bypass the control-plane countermeasures and then targets the data-plane (i.e. the part where routers forward data packets along the computed paths). Therefore, the adversary can drop, modify, re-order, delay or misdirect data packets. Moreover, he can corrupt forwarding tables to meet his needs or install access control lists that arbitrarily or selectively misdirect data traffic to a route which is not the best or could even be the worst, leading to so-called *misdirection attack*. However, cryptographic mechanisms alone cannot prevent such data-plane attacks since many of them such as misdirection attack can be launched without the need to decrypt cipher data or having access to cryptographic keys.

In this thesis, we focus on the misdirection attack launched in data-plane phase and propose a lightweight, efficient and secure route authentication and misdirection detection (RAMD) protocol to authenticate the forwarding routes before delivering data, and detect malicious routers that could misdirect traffic within autonomous systems that apply link-state routing protocols such as OSPF. In our protocol design, we adopt hybrid approach that involves active probing and filtering techniques, where a router sends a probe packet to authenticate the route before delivering data and then builds a filtering table to detect misdirected data packets.

Our protocol doesn't require cryptographic operations at data-plane phase and imposes a very little computation, communication and storage overhead. Moreover, it's able to detect and respond to both passive and active misdirection attacks. We believe our work is an important step in detecting and preventing misdirection attack.

ملخص

لقد صممت الانترنت في الاصل لتعمل ضمن بيئة موثوقة ومعتمدة وقابلة للتوسع، كما أن البنية التحية لها وبالأخص أنظمة التوجيه (Routing Systems) لم تعتمد نظام الأمان عند تصميمها، فقد اصبحت أجهزة التوجيه عرضة لهجمات لا تستهدف المستخدم فقط، بل تؤثر بدورها على اداء الشبكة كله. أحد هذه الهجمات هو قيام الهاكر باختراق جهاز التوجيه ومن ثم ترك مستوى التحكم (Control-Plane) – هو الجزء الذي تستخدم فيه أجهزة التوجيه البروتوكولات الخاصة لتبادل رسائل التحديثات والتحكم (Updating Messages)، الخاصة باكتشاف هيئة الشبكة وحساب أقصر الطرق بين أجهزتها– ليعمل بشكل صحيح حتى يتمكن من تخطي إجراءات الحماية لمستوى التحكم بقصد استهداف مستوى البيانات (Data-Plane)- هو الجزء الذي تقوم فيه أجهزة التوجيه بتمرير حزم البيانات بناء على أقصر الطرق التي تم حسابها في مستوى التحكم. هكذا يبدأ الهاكر بالهجوم على حزم البيانات بأن يقوم بأحد هذه العمليات: الحذف ،التعديل ، إعادة الترتيب، التأخير أو توجيه حزم البيانات الى مسار خاطئ.

ان الهاكر يستطيع العبث بجداول التوجيه أو تثبيت بعض قوائم التحكم التي بدورها تغير المسار الصحيح للبيانات بشكل انتقائي أو بشكل تعسفي مما يؤدي الى ما يسمى "هجوم التوجيه الخاطئ" (Misdirection Attack). من ناحية أخرى، فان آليات التشفير وحدها لا تمنع مثل هذا الهجوم، لأنه يمكن أن ينفذ دون الحاجة إلى فك تشفير البيانات أو امتلاك مفاتيح التشفير السرية.

في هذه الأطروحة، قمنا بالتركيز على حل مشكلة هجوم التوجيه الخاطئ الذي ينفذ في مستوى البيانات، واقترحنا بروتوكول: التحقق من صحة المسار واكتشاف هجوم التوجيه الخاطئ Route Authentication and Misdirection Detection (RAMD) حيث يقوم البروتوكول بالمصادقة على صحة المسار قبل ارسال البيانات اضافة لاكتشاف أجهزة التوجيه الخبيثة التي توجه البيانات بشكل خاطئ في اطار الشبكات ذاتية التحكم التي تطبق بروتوكولات التوجيه المعتمدة على حالة الارتباط (Link-State Routing Protocols) مثل بروتوكول OSPF . بشكل عام هذا البروتوكول يضيف عبئا ومساحة تخزين على أجهزة الشبكة بشكل ضئيل جدا ، إلا أنه آمن وفعال.

لقد اعتمدنا في تصميم هذا البروتوكول نهجا ينطوي على التكامل بين تقنية الجس النشط (Active Probing) وتقنية التصفية (Filtering) بحيث يرسل جهاز التوجيه حزمة الجس، التي تتأكد من صحة المسار قبل ارسال البيانات ومن ثم تبني جدول التصفية لكشف الحزم التي تسير في مسار خاطئ.

البروتوكول المقترح يستطيع الرد على هجمات التوجيه الخاطئ السلبية (Passive Attack) والفعالة (Active Attack) على حد سواء مع أنه لا يتطلب اجراء عمليات تشفير أثناء ارسال حزم البيانات، ان بروتوكول (RAMD) هو خطوة مهمة نحو اكتشاف ومنع هجوم التوجيه الخاطئ.

Table of contents

1.1 Introduction

Today, the rapid growth of the internet and continuing increase of many critical services such as web applications (e.g. e-mail and e-commerce) and real-time applications (e.g. Video conferencing and voice over IP (VoIP)) depend mainly on the internet infrastructure to provide them with reliable, efficient and secure communications. However, the routing infrastructure was not constructed with security in mind. Rather, the routing protocols that the internet is based on were originally designed to operate in a completely trusted and open environment assuming no malicious nodes or attacking behavior. As a result, routers are subject to malicious attacks targeting not only a single subnet or individual user, but also the overall network performance [2], [3].

In addition, the routers are designed to operate at the network layer. So, attacking on this layer can cause malfunctions of the entire routing domain regardless of what services, devices or users are operating. Therefore, the importance of securing the routing infrastructure has grown rapidly and becomes a significant issue.

In general, attacks on the routing system can be launched either in the *control-plane* which is the part where routers apply the routing protocols to exchange control and update messages that discover the network topology and compute the shortest paths, or in the *data-plane* which is the part where routers forward data packets along the computed paths [14]. These attacks are generally described in the IETF Internet draft [4].

Much research has focused on securing routing infrastructure by implementing countermeasures in the control-plane as in [9-13]. However, the researches [15], [17] show that simply securing the control-plane is insufficient to secure data forwarding. For example, an adversary could compromise a router (we refer to this compromised router as a malicious),

routing protocols operate properly in order to bypass the control-plane countermeasures and then targets the data-plane. Therefore, the adversary can drop, modify, reorder, delay or misdirect data packets. Moreover, he can corrupt forwarding tables to meet his needs or install access control lists that arbitrarily or selectively misdirect data traffic to a route which is not the best or could even be the worst, leading to so-called *misdirection attack*. As a consequence, misdirection attack results in significant network performance degradation, in particular, for critical applications (e.g. real-time applications), in addition to causing deliberate security violation by misdirecting traffic to a black-hole or monitoring point, besides, disrupting network availability through denial-of-service (DoS) attack [8].

An example of traffic misdirection attack is illustrated in figure1.1. Assume the shortest route from **A** to **I** is: **A-B-E-H-I** which is initially calculated by router **A** using Shortest Path First (SPF) algorithm (e.g. Dijkstra algorithm [5]). If router **E** is being malicious, it may misdirect the traffic to an invalid route **A-B-E-F-G-I** which is not the shortest or optimal route.

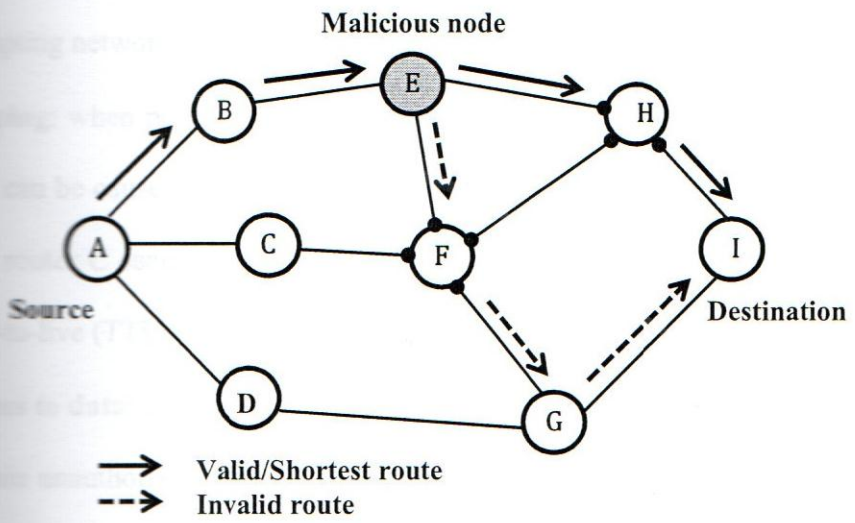

Figure 1.1: An example of traffic misdirection attack.

In general, the impact of traffic misdirection attack may include [7]:

- **Sub-optimal routing**: here, the main objective of the attacker is to misdirect incoming traffic to increase latency. In real time applications such as video streaming and VoIP, the performance of the network is a critical issue. So, misdirection attack may cause the traffic to traverse on sub-optimal paths that are either congested or longer than the optimal or shortest paths. As a result, the network performance will be degraded leading to unsatisfactory performance of critical applications.
- **Congestion**: flooding a specific route with high traffic will lead to so-called artificial congestion. So, the data could be lost as routers connecting the congested link will drop packets. However, this artificial congestion will not be solved by traditional control mechanisms.
- **Host overwhelming**: by misdirecting numerous numbers of packets to a victim node, this node will become overwhelmed and the running services will be no longer available. Moreover, the attacker may cause the system to shut down and thus prevent legitimate users from using system services. Therefore, traffic misdirection will lead to DoS by disrupting network or service availability.
- **Looping**: when packets are misdirected to incorrect paths then the looping may occur. This can be caused when router A sends data to router B, which sends data to router C, then router C sends data back to router A. Therefore, this loop will continue until the time-to-live (TTL) value expires in TCP/IP.
- **Access to data**: a malicious router can misdirect data traffic to other nodes that benefit it to gain unauthorized access to data which would otherwise be inaccessible by original routing path.

- Accusing **well-behaving nodes as malicious**: here, the malicious router misdirects traffic arbitrarily to a well-behaving neighbor to overwhelm it. While it gives the impression to its neighbors that it performed the legitimate forwarding action. As a result, this overwhelmed router will drop packets due to buffers overflow. Therefore, misdirecting may cause well-behaving routers to appear as malicious routers as they unintentionally drop data.

On the other hand, cryptographic mechanisms alone cannot prevent such data-plane attacks since many of them such as misdirection attack can be launched without needing to decrypt either data or having access to cryptographic keys. For example, the IPsec [31] is commonly used to provide end-to-end cryptographic protection at the network layer. It can help guard against packet modification, analyzing and replaying. Nonetheless, it's powerless against the malicious nodes that attempt to drop or misdirect packets [37]. However, many approaches have been proposed over the years to defend against data-plane attacks, in particular, the misdirection attack. While some of these approaches are not specifically designed for solving the misdirection problem, they suffer from certain shortcomings such as high computation and communication overhead or high storage requirements. These approaches are discussed in detail in Chapter 3 where we discuss a large number of currently proposed solutions.

In the light of what is mentioned above, the main goal of this study is to develop a lightweight, efficient and secure protocol to defend against traffic misdirection attack launched in data-plane phase. This protocol is aimed at detecting faulty or malicious routers that misdirect data traffic and then respond to these faulty routers by removing from routing fabric and dealing with them.

On the other hand, we select the link-state routing protocols (e.g. Open Shortest Path First (OSPF) protocol [1]) as an underlying routing protocol for our protocol design. A quick

overview of OSPF and the advantages that encourage us to choose the OSPF as an underlying protocol are presented in next section.

A brief Overview of OSPF Protocol

OSPF is an interior gateway protocol or intra-domain routing protocol, which is designed to route traffic within a single autonomous system (AS). Whereas, the protocols that are designed to route traffic between AS's are called exterior gateway protocol or inter-domain routing protocol such as border gateway protocol (BGP) [32]. OSPF is a widely deployed link-state routing protocol. Its fundamental concepts can be summarized as follows:

OSPF use the link-state paradigm to compute shortest routes between routers. In link-state routing, each router discovers its neighbors and the corresponding weights (costs) of the links connecting them, and then floods this information by a reliable link-state advertisement (LSA) messages to the routing area. When a router receives LSA from a neighbor, it retransmits this information to all other directly connected neighbors. Each router uses these LSAs to build the link-state database (LSDB) which provides a complete image about the entire structure of the network topology. With this database, each router can recognize the internal network topology and calculate the shortest path to every other router using Dijkstra algorithm [5]. When the network topology or the state of a link is changed (e.g. link comes up/down), the affected routers will flood appropriate LSAs to notify the entire network to update their LSDB and maintain the same LSDB with all other routers. However, the two main advantages that encourage us to choose OSPF as an underlying protocol are:

1. Each router can calculate the shortest path between any two nodes in the network and recognize the nodes sequence between the source and the destination.

2. Each router can recognize the address spaces (networks prefixes or connected subnets) of other routers and construct a complete image of internal network topology.

For any further information about OSPF operation and design, the reader can refer to [1].

1.2 Thesis Contributions

To achieve the main goal of this study, we have developed a new protocol called route authentication and misdirection detection (RAMD) protocol to defend against the misdirection attack launched in the data-plane. In our protocol design, we adopt a hybrid approach that integrates both active probing and filtering techniques. In general, the active probing techniques [17-19] aim at discovering the forwarding routes by sending test (probe) packet to check for consistency with advertised routes, and then detecting the packet forwarding misbehavior. While the filtering techniques [20-22] is a process of filtering out packets based on their source and/or destination addresses for the purpose of detecting the IP-spoofed packets or the packets that don't fulfill the pre-defined rules of the routing protocols. So, our protocol employs probe packets (called route authentication packets (RAP)) in order to authenticate the shortest routes before delivering data and then updates the filtering tables (called route authentication tables (RAT)) at every router along the selected route to detect the misdirected packets. Therefore, if the route is authenticated, then the misdirected packets will be detected by the RAT and the malicious routers that misdirect traffic will be addressed accordingly.

The contributions of this thesis can be summarized as follows:

1. We develop the RAMD protocol to defend against traffic misdirection attack launched in data-plane phase. This protocol is designed to operate within AS's. The link-state routing protocols (e.g. OSPF) are selected as an underlying protocols. The major advantages of

6.1 Conclusions

The routers are target of many attacks launched in both control-plane and data-plane. In control-plane, the goal of an attacker is to disrupt the routing protocol by falsifying the update messages or impersonate other routers. In data-plane, the attacker can launch more subtle attacks such as dropping, reordering, delaying and misdirecting packets. However, cryptographic mechanisms alone cannot prevent these attacks since many of them, such as misdirection attack can be launched without the need to decrypt cipher data or having access to cryptographic keys.

In this thesis, we study the misdirection attack problem and present the RAMD protocol to detect the misdirection attack launched in data-plane phase. Our protocol is designed to operate within autonomous systems that apply link-state routing protocols such as OSPF.

The RAMD protocol adopts hybrid approach that involves probing and filtering techniques where the router should authenticate the route before sending data by initiating route authentication process and then build RAT to filter out the misdirected data packets. In addition, our protocol employs an effective scheme called fault-coding scheme to detect faulty links and faulty routers. Moreover, it can respond to detected faulty routers by removing them from routing fabric to stop dealing with them and avoid packets to pass through unauthenticated routes. According to our analysis, the advantages of RAMD protocol can be summarized as follows:

- *Secure*: it uses the MAC to authenticate the RAP and securely update the RAT.
- *Lightweight*: it imposes very light communication, computation and storage overhead. Firstly, to reduce the computation overhead, RAMD protocol avoids using online cryptographic operations and doesn't require the computation of fingerprints or MAC