TrustR: Protecting Computer Networks using Router security framework Integration

Mrs. Smita Samrat Mande
Department of Computer Engineering
AISSMS IOIT, Pune

Abstract- *The seriousness and number of attacks on computer networks are increasing substantially. Most existing security solutions focus on avoiding one or more attacks. We propose an integrated router security framework, called TrustR. It is able to resist against various types of attacks. TrustR combines security primitives including cryptography based security mechanisms, trust management system, and trusted platform module. A simple and efficient method for detecting deceptive routing messages is also proposed. The deployment of TrustR is introduced.*

Keywords- Cryptography, Deceptive Routing, TrustR, trust management

I. INTRODUCTION

With The Fast development of network-based technologies such as Internet and ubiquitous computing, computer networking becomes increasingly pervasive and necessary. As the core device, routers are responsible for connecting different networks and forwarding data packets. In addition to dedicated router device, end nodes in networks such as ad hoc networks also act as routers.

In spite the great significance of computer networking, it has also used as a vehicle for various security attacks [1]. The router is rather vulnerable because of its critical role. The functionality of a router can be divided into data plane, control plane and management plane [2]. Accordingly, attacks can be categorized into three types: 1) unauthorized access to network resources, such as IP address spoofing; 2) data-plane attacks to prevent data packets from being successfully delivered, such as BlackHole and JellyFish [3]; 3) control-plane attacks to disturb or disrupt network operations, such as routing spoofing.

To block unauthorized access, many cryptographic authentication schemes have been proposed [4]. These methods are based on the foundation that authenticated entities are absolutely trusted because intruders cannot get authenticated. However, emerging attack techniques, such as advanced persistent threats and social engineering attacks, break up the foundation. By changing the compromised router systems, intruders can bypass the cryptographic mechanisms. Then, more internal attacks could be introduced. Fortunately, trust management system has been introduced as the second wall. Trust is the degree of belief about the future behaviors of other entities [5]. The behaviors of a node can be reflected by some metrics called trust factors, such as packet delivery ratio (PDR). According to trust factors, a trust value denoting the trustworthiness degree of the node is evaluated by a trust evaluation model. Then other nodes can decide whether to interact with this node according to its trust value. Trust-based security mechanisms are able to detect and defend those malicious authenticated nodes as long as they misbehave.

Although substantial trust-based solutions have been proposed [6], [7], there are still some problems which are unsolved, particularly the difficulties in collecting trust factors for securing networks. Cryptographic approaches and trust management systems are effective in resisting unauthorized access and data-plane attacks, but countering the control-plane attack is still challenging. Two popular methods, rule-based method [8] and detecting-message-based method [9], are used to deal with control-plane attacks. The rule-based method finds out whether a received routing message follows the routing protocol specification according to a set of predefined rules. However, it is very difficult to define reserved rule set. The detecting-message-based method sends specific messages to suspicious nodes. According to the feedback, a node can judge whether the suspicious node violates routing protocols.

To protect computer networks from all three types of attacks, the following security requirements should be satisfied: 1) control messages, particularly the routing messages, should be authenticated; 2) routers not forwarding packets as expected should be excluded from routes; 3) correctness of routing messages should be verified before handled or before sent, and FIB should also Host Router
be verified before used; 4) the security system should be self-protected.

To fulfill these requirements, we propose an integrated router security framework, called TrustR. Its advantages are: 1) It is able to resist against all three types of attacks, which is benefited from the four independent but cooperative components, i.e., the cryptography based security

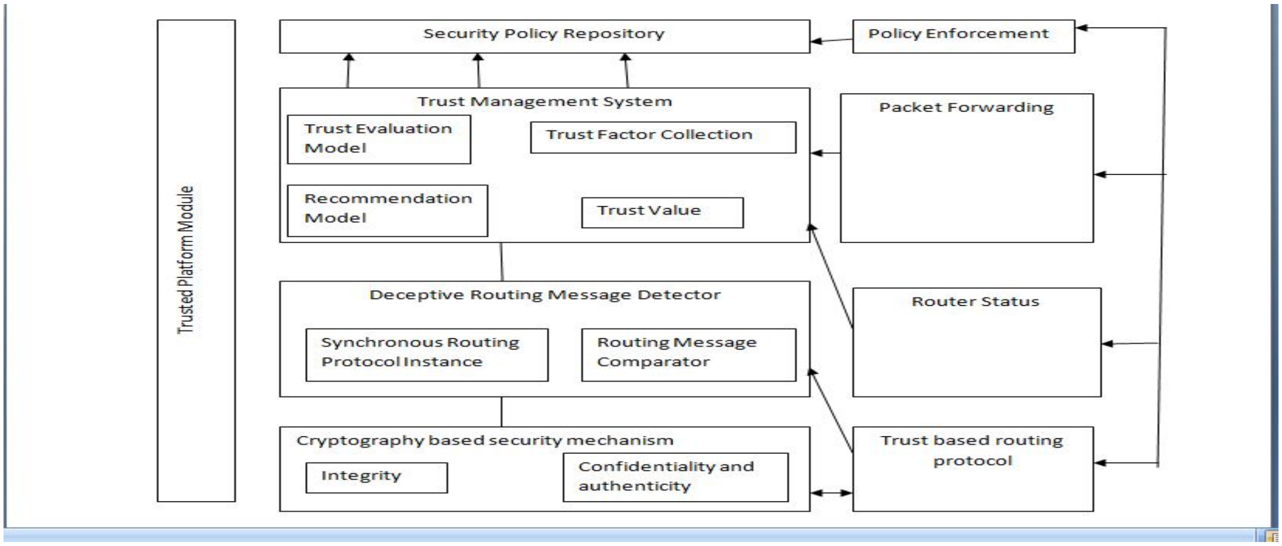
Trusted Platform Module
Security Policy Repository
Policy Enforcement
Trust Management System
Trust Evaluation Model
Trust Factor Collection
Recommendation Model
Trust Value
Packet Forwarding
Deceptive Routing Message Detector
Synchronous Routing Protocol Instance
Routing Message Comparator
Router Status
Cryptography based security mechanism
Integrity
Confidentiality and authenticity
Trust based routing protocol

Fig 1. TrustR Framework

mechanisms, the deceptive routing message detector, the trust management system, and the trusted platform module (TPM); 2) A simple but efficient method to detect deceptive routing messages and FIB is proposed and built in TrustR.

II. TRUSTR FRAMEWORK

The framework of TrustR along with the related units of the host router are shown in Fig. 1. TrustR meets all the security requirements described in section I due to the multiple integrated components, as elaborated in the following. From the perspective of the host router, TrustR performs as an independent trusted third party installed on it.

A. Cryptography Based Security Mechanisms (CBSM)

The first thing external attacker would do is to intrude into networks. If no security mechanisms like authentication and access control are applied, the attacker can participate in the networks directly. Otherwise, attacks such as IP address spoofing and Man-in-the-middle would be launched. The most efficient way to detect external attacks would be cryptographic methods that support identity and message authentication, confidentiality and replay protection. A typical example is the Internet Protocol Security (IPsec) protocol suite. After applying such mechanisms, each node is verified before accessing networks, and control messages are authenticated before handled. As a result, the unauthorized intruders will be warded off. In TrustR, the cryptography based security mechanisms can be any proper security protocols or security extensions to current protocols. All received control messages should be authenticated inside TrustR before given to the host router. Likewise, fields such as Message Authentication Code (MAC) should also be calculated inside TrustR.

B. Deceptive Routing Message Detector (DRMD)

Routing protocol is responsible for creating paths to pass the packets. Although external intruders could be warded off by CBSM, internal malicious or compromised routers can still propagate deceptive routing messages to disturb or disrupt networks. As is well known, routers use FIB to forwards packets in the data plane. FIB is updated according to the routing table in the control plane. A smart attacker may not misbehave in the control plane to avoid being detected, but it could produce an Incorrect FIB. Simultaneously the router would not forward packets correctly. To prevent deceptive routing messages, a replicated routing protocol instance is deployed inside TrustR. This instance is synchronous with that in the host router. The synchronization is possible because TrustR is between the host router and networks, and thus it is able to receive the same routing messages as the host router receives. A comparator is then used to compare the out coming routing messages produced by the two instances. If they are identical, this message is considered correct and sent to networks. Otherwise, the message will be ignored and this host router will be suspected malicious.

C. Trust Management System (TMS)

CBSM and DRMD are effective in resisting unauthorized access and control plane attacks, but not in countering data plane attacks such as BlackHole, JellyFish and Denial of Service. It is difficult to detect them because they usually do not violate protocol specifications. Trust management provides a dynamic way to detect and Avoid data-plane attacks. The malicious nodes which often have low trust value are excluded from routes during routing calculation. The trust factors of TMS protecting computer networks could include packet loss rate, average delay, and router status such as load, energy and mobility. In existing TMSs, a router is often monitored and evaluated by its neighbors. This means certain neighbors should Collect trust factors of the router. In wireless networks, the common approach is eavesdropping [10]. In fixed networks, extra devices can be deployed to monitor traffic flows [11]. Both of them cannot perceive router status information, and the Collected information may not be exact enough. While in TrustR, the collection becomes easy, because TrustR is deeply integrated into the host router and able to Access certain information directly. For instance, it can read the router status information from hardware. This not only facilitates the collection, but also assures the correctness of the collected trust factors. Note that any proper trust models can be integrated into TrustR. In addition, the security mechanisms that protect trust Management systems from attacks, such as collusion attacks, can also be included in TrustR.

D. Trusted Platform Module

TPM is employed to protect the TrustR itself from compromised. TPM is a dedicated microprocessor designed to secure computer systems by integrating cryptographic keys. It has been widely used in assuring device integrity, password protection, disk encryption and digital rights management etc. In TrustR framework, it mainly assures the integrity of each component, store keys to keep them inaccessible to external programs, and complete encryption and decryption.

E. Security Policy Repository

After detecting a compromised host router, TrustR may produce instructions to recover it, e.g., reset it back to the normal state. These instructions may involve multiple parts of the router system. Executing them in an individual way may greatly increase the system complexity. To avoid this, all instructions are first translated into security policies with uniform format, and a repository is then established to cache these policy items. Accordingly, a policy enforcement interface that translates polices into instructions and executes the instructions should be added to the host router.

III. CONCLUSION

In this paper, a TrustR framework for protecting computer networks is proposed. It integrates several security technologies to defend various types of attacks. A simple and efficient method for detecting deceptive routing messages is proposed.

REFERENCES

[1] A. K. Abdelaziz, M. Nafaa, and G. Salim, “Survey of routing attacks and countermeasures in mobile ad hoc networks,” in Proc. UKSim, 2013, pp. 693–698.

[2] A. Greenberg et al., “A clean slate 4D approach to network control and management,” ACM SIGCOMM Comp. Commun. Rev., vol. 35, no. 5, pp. 41–54, Oct. 2005.

[3] I. Aad, J.-P. Hubaux, and E. W. Knightly, “Impact of denial of service attacks on ad hoc networks,” IEEE-ACM Trans. Netw., vol. 16, no. 4, pp. 791–802, Aug. 2008.

[4] A. Alomari, “Security authentication of AODV protocols in MANETs,” in Proc. Netw. Syst. Secur., 2013, pp. 621–627.

[5] S. Tan, X. Li, and Q. Dong, “Trust based routing mechanism for securing OSLR-based MANET,” Ad Hoc Netw., vol. 30, pp. 84–98, Jul. 2015.

[6] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, “A cooperative routing for manet based on distributed trust and energy management,” Wireless Pers. Commun., vol. 81, no. 3, pp. 961–979, 2015.

[7] O. A. Wahab et al., “A survey on trust and reputation models forWeb services: Single, composite, and communities,” Decis. Support Syst., vol. 74, pp. 121–134, Jun. 2015.

[8] A. Adnane, C. Bidan, and R. T. De Sousa Junior, “Trust-based security for the OLSR routing protocol,” Comput. Commun., vol. 36, no. 10–11 pp. 1159–1171, 2013.

[9] M. Marimuthu and I. Krishnamurthi, “Enhanced OLSR for defense against DOS attack in ad hoc networks,” J. Commun. Netw., vol. 15, no. 1, pp. 31–37, 2013.

[10] Z. Wei et al., “Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning,” IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 4647–4658, Nov. 2014.

[11] T. Han et al., “Study on security routing algorithm based on dynamic adjacent trust,” J. Commun., vol. 34, no. 6, pp. 191–200, Jun. 2013.