A Survey paper on Wireless Router: Attacks and Defenses

Shriya Raviprasad, Saparbek Nagashibekov, Mahak Malik

Abstract: *The router has become the primary control point in the increasingly complex network environment, holding responsibility for service quality and security, monitoring and efficiency, and other attributes that allow networks to add value. We present the timeline of attacks and defenses on the routers and this will give an idea to future research workers on which direction they must invest their time to secure the router infrastructure.*

Introduction:

Routing is the hub around which all of IP connectivity revolves. At the simplest level, routing establishes basic internetwork communications, implements an addressing structure that uniquely identifies each device, and organizes individual devices into a hierarchical network structure. Traditionally, routers have also served as the media adapters that have connected remote offices to the headquarters via a WAN. The most recent trend, though, is to see routers as the integration platforms for a wide variety of network enhancements such as security, policy, and services that extend the capabilities of IP to support telephony, video, legacy service integration, and other applications over a converged network. This means the router has become the primary control point in the increasingly complex network environment, holding responsibility for service quality and security, monitoring and efficiency, and other attributes that allow networks to add value. We present the timeline of attacks and defenses on the routers and this will give an idea to future research workers on which direction they must invest their time to secure the router infrastructure.

Timeline of Attacks and Defenses:

The paper A Scalable Method for Router Detection and Location in Link State Routing was published in **2003** and this paper authors addressed the one of the well-known attacks i.e. router table poisoning attack. The routing table is a crucial link as it is used to decide the route for transferring of packets. So, if a malicious router makes the other nodes update their database with a false route then it can lead to packer drop or blocking of a route.

In earlier days, **2004**, there were attacks where a malicious router misroutes the packets so that triangle routing is formed. This kind of attacks is very difficult to detect, and the problem was considered as an open problem. There were two kinds where the packet misrouting could be achieved. One was static routing where the router is assumed to have been compromised and the routes are modified. And another is access control lists where the routes are modified based on time intervals.

In 2012, a new Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router was proposed [1]. The WLAN security standard applies this authentication method to prevent a security threat such as hacking using rogue APs (Access Point). In this authentication method, RADIUS servers authenticated APs using static shared secrets. However, this method was not suitable for WLAN environments where mobile routers are used [1]. Mobile routers are always exposed to device hacking and thus they are subject to very high risks of the leak of shared secrets. Therefore, they require secure authentication methods. Park et al. (2012) proposed a new IEEE 802.1x based authentication method of which the security has been enhanced using Trusted Platform Module (TPM) [1]. The proposed method involved no risk of authentication key leaks at all and can fundamentally block any attempt of hacking using rogue APs as the server verifies the integrity of APs in the process of authentication [1].

The proposed method has enhanced the security of the IEEE 802.1x based authentication method [1]. It does not use the static shared secret in authentication between RADIUS servers and APs but

applies a new device authentication method using TPM. The proposed method has been enabled to authenticate APs of which the access is requested by the server using the Endorsement key (EK) and RTR (Root of Trust for Reporting) function of TPM as well as verifying the integrity of the Aps [1]. Furthermore, it has been made to encrypt Master secret key (MSK) generated through mutual authentication between the user device and the server using a public key of the TPM when the MSK are delivered to the AP so that the MSK can be decrypted using only the TPM [1].

In the proposed method, only those APs that have been registered in the server in advance can be authenticated by the server to provide WLAN services [1]. Therefore, all APs should be registered with the server through specified procedures. The proposed method is composed of a process to register APs to servers and an IEEE 802.1x based authentication process using registered APs. In AP initialization and registration procedure, for a WLAN AP to be authenticated by a RADIUS server, the Attestation Identity Keys (AIK) of the TPM should be generated and then the certificate of the AIK should be registered with the server [1]. This process is as shown in Figure 1.

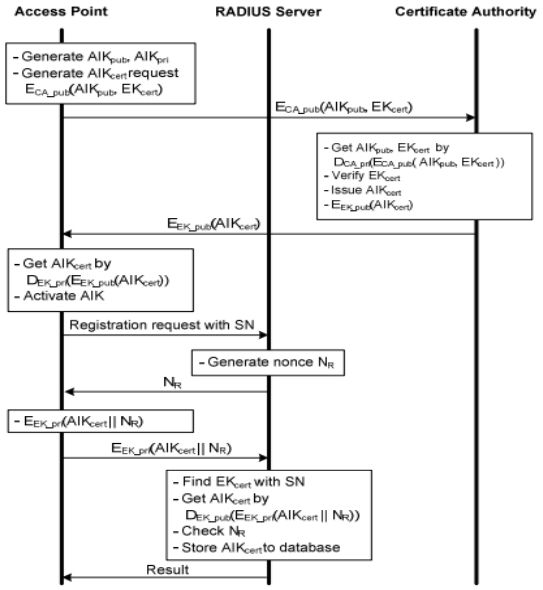

Figure 1. Access Point initialization and registration procedure [1].

An AP initializes its TPM and generates an AIK asymmetric key pair. Then, it requests the Certificate Authority(CA) to issue a certificate for the generated AIK. In this case, the AIKpub, the public key of the AIK and the EKcert, the certificate of the TPM are encrypted with the CA_pub, the public key of the CA and the result, ECA_pub(AIKpub, EKcert) is transmitted to the CA to request for the issuance of the certificate [1]. Then, the CA verifies the message transmitted by the AP requesting for the issuance of the certificate and issues AIKcert, the certificate of the AIK.

The proposed authentication method provided a higher level of security [1]. In this method, only those APs registered with the RADIUS server in advance and verified for integrity can provide WLAN services [1]. The server verifies the attestation value presented by the AP requesting for access to authenticate the AP. That is, the server compares the Na obtained by decrypting the attestation value generated by the TPM of the AP with the Na possessed by it to see if they are the same to check whether the AP has been registered in advance and verifies the integrity of the AP by comparing PCRs values. In addition, the proposed method encrypts the EK_pub of the TPM with a key in the process of delivering the MSK generated through mutual authentication between the user and the server to the AP [1]. The EK_pri of the TPM exists only in the TPM. Therefore, the encrypted MSK can be decrypted by only those APs registered with the server. Therefore, this method provides a higher level of security compared to methods where anybody that knew shared secrets could decrypt MSK [1].

In conclusion, the proposed IEEE 802.1x based authentication method with enhanced security applied the RTR function of TPMs to authentication procedures between APs and servers so that the integrity of the APs requesting access is verified [1]. The method was made to authenticate APs using EKs, unique keys of TPMs to safely deliver MSKs generated through authentication to APs. Therefore, by applying the proposed method, MITM attacks using rogue APs can be fundamentally blocked. However, the proposed method does not require any change in WLAN user devices. In addition, since TPMs provide most software toolkits necessary for its application even though they are cheap and thus the proposed method can be applied easily at low costs.

In 2013, Router attacks detection through log analysis and defense mechanism method was proposed [2]. A router is one of the most important devices in networking. It plays a significant role in

communication in the campus. A router can be attacked in many ways by a hacker. Most commonly, Distributed Denial of Service Attack can hit the router. Routing packets between networks is the main aim of a router. Many Man in the Middle (MiM) attacks can be caused which will direct the traffic to an attacker instead of sending it to the legitimate router [2]. Therefore, a network administrator must monitor the router for its security. Using logs of routers is the best way to monitor any system, and it can help to detect many serious attacks. However, routers have very less memory to store logs. Thus, Waichal et al (2012) proposed to direct router's log to a separate Syslog server, for attacks detection [2]. This also provides a clean separation. The router console will not be interrupted with logs. Apart from all above techniques, proper log analysis of logs can give a lot of insight in attacks detection. After attacks are detected, a mechanism is also stated to configure appropriate access list (ACL) on the router as a defense mechanism [2].

Implementation of the proposed system is not difficult. Firstly, it is necessary to configure the router to direct logs to another host (Syslog server) [2]. After that, the logs can be viewed on the separate machine having Syslog server. Log analysis can now be done on this machine. The most appropriate place for deploying the Syslog server and the log analyzing program would be as shown in Fig. 2 [2].

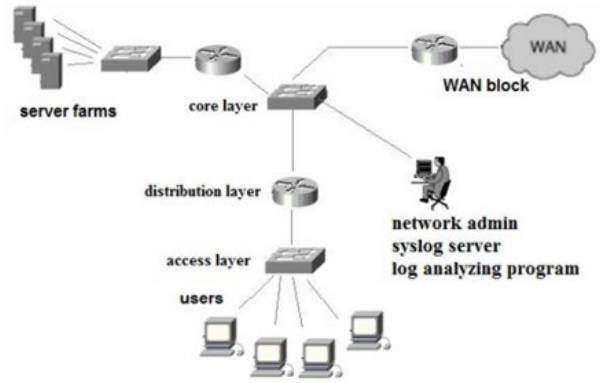

Figure 2. Deployment of Syslog Server in Campus Network [2].

As shown in Figure 2, the machine on which the Syslog server is running is connected to the core switch. In this way, all the routers can direct their logs to the Syslog server. This gives the network administrator control over monitoring all the routers [2].

Along with the Syslog server, few other modules can be deployed on the system. For example, there are modules such as File Processing, Attack detection, and Communication with the router. File processing module will divide the single Syslog file into separate files according to the protocol. This step is critical because it is beneficial for attacks detection where networking administrator will analyze the flow of activities inside a protocol. For example, OSPF (Open Shortest Path First protocol) activities can be monitored easily from the OSPF log file [2].

Attacks Detection and Communication with the router modules are the essential part of the proposed system. Some attacks can be detected by just analyzing one log entry such as BGP's session termination attack or ICMP redirect attack [2]. On the other hand, some attacks require analyzing more than 1 line before declaring that an attack has happened. Communication with the router module has 2 main reasons for having it. 1. Turning ON all possible logging is not recommended on the routers because it will slow down its operation. So, if in case, the network administrator wants to monitor only routing protocols for some time, then the software will give a menu item to turn ON debugging only for OSPF, BGP etc. [2] 2. After an alert for some attack is raised, its defense mechanism must be started [2]. The network administrator will usually take all efforts to prevent any attack happening on the router in the first place. Yet unfortunately, if any attack occurs then its defense mechanism should be initiated.

To conclude, this proposed system, Syslog server for attacks detection is a complete network monitoring tool. It will tell about all the working protocols on the routers. This system has found a way to dump log to separate machine and sort them. It can fire commands on the router which means it can easily obtain the output of 'sh run' from routers. Furthermore, it knows how to extract information from the log to detect an attack. It has also defended routers by configuring ACLs.

In the same year, **2013**, another paper gave a survey of different methods for router management and security. The aim was to detect any anomalous

behavior of router which can lead to collapse of entire network. It then focused on using an excellent in-built feature available in almost any machine-like router or web server or mail server or switch or database server which is logs. Proper analysis of logs that are generated can be extremely useful for detecting any anomalous behavior of the router. Thus, they proposed a mechanism where logs can provide huge information for solving a misconfiguration on router or detect an intrusion on the system. In this paper they provided details about how to use router logs for attacks detection and defense.

There were many other attacks launched, like built-in back door attacks. Vendors often include remote administration features in router firmware for faster development and debugging. In some cases though, these features are not removed prior to the product's release. Users are therefore not aware of their existence. Some vendors claim that the inclusion of these features are for emergency updates. Still, attackers may abuse them for nefarious purposes and use them as "built-in backdoors."

In 2014, a backdoor was found in the WAN part of the Netis/Netcore routers3 that allowed attackers to access, and consequently, compromise routers through the execution of arbitrary commands and by making the routers susceptible to man-in-the-middle (MitM) attacks. Months after this backdoor vulnerability was reported, Netis/Netcore released firmware updates.4 Although the update closed theport, the backdoor codes remained.

Cisco also had its own share of backdoor trouble with its SYNful Knock implant.5 Any attacker can runfunctional modules and change the Cisco IOS image with this. On the other hand, certain versions of D-Link's router settings6 can be accessed and modified through a backdoor. With this, attackers can redirect users to malicious pages and phishing sites.

Another attack was presented in **2015** by the authors of owning of home router such as XSS, CSRF and UI redressing. All these attacks are quite common in today's world. These can be used to take access of the router through getting the credentials of the admin page of the router. Another attack known as Krack i.e. key reinstallation attack can be used to do the man in the middle attack. Currently all the devices that work on Wi-Fi are affected by this vulnerability.

The solution for preventing routing table poisoning is secure link state routing protocol(SLIP). This protocol consists of two parts i.e. consistency and synchronization. In the consistency check the protocol has three data structures i.e Ajacency matrix in which the weight of route between two nodes is given second is suspicion matrix, in this any change to the routing table is added to this matrix before the validation, and the last is malicious list, which contains the nodes which have publicized the false routes. Along with these three lists the protocol also as suspicious timer T(i-j), which is set when a new route is publicized between node I and j.

Another part is synchronization check. It is carried out using principle of voting. the first principle is that each node receives information from each of its nodes. Second, each entry I of the adjacency matrix I th element comparison is done, thirdly, the entry which has maximum votes is kept, forth, in case of a tie, the original entry is kept. Finally, the suspicious matrix nodes are excluded.

As for the defense of Krack attack, a new protocol such as WPA3 is in progress. The only way to prevent from this attack is an update to the Wi-Fi protocol i.e WPA2.

In **2016**, Trend Micro Labs Research Team published a paper. Their focus was on a bigger problem called Mirai. When Mirai first came into the picture, it dispelled the notion that the attack scenarios on Internet of Things (IoT) devices were merely a proof of concept (PoC). After all, Mirai's widespread attacks on organizations and users revealed how vulnerable IoT devices, like home routers and IP cameras, can be abused for cybercriminal activities.

In 2017, In order to solve issues related to drawbacks of the hardware device, Chaitra and Sharma (2017) proposed the integration of Software Router with Wi-Fi for Enhanced Security system [3]. The hardware routers and firewalls have drawbacks. They are two individual devices with unique features to provide a secure network. There are diverse firewall connections, which have different configurations of the network [3]. According to the needs of the organization, required firewall devices are purchased.

However, in case an organization needs to modify the functionality of the firewall, the configuration on the existing firewall cannot be changed, as it is a closed system i.e. source code cannot be altered [4]. Hence, the firewall with the required modifications must be purchased again, which is not cost effective [4]. One of the disadvantages is that it requires the high amount to be invested as the number of hardware devices increase, and hence lacks scalability. Investing in the same type of devices might also not provide full-fledged functionalities such as security to confidential data, blocking websites, securing websites from hackers and proxy servers. Therefore, the Vyatta software router was proposed, which includes both router and firewall configurations to overcome the drawbacks of the hardware device [3]. Running a firewall (hardware) on both a router as well as a computer can provide multiple lines of defense when it comes to dealing with attacks [4]. However, separate hardware devices for router and firewall lack security [5]. User credentials can be hacked, as these details are not encrypted with security standards in Wi-Fi such as wired equivalent privacy (WEP), WEP II, and wireless access protocol (WAP), leading to loss of confidential information [5]. User credentials can be noted and encryption techniques can be identified by regular notice of data [3].

The integration of the Vyatta software router with Wi-Fi module and firewall device provides high performance, scalability, and security [3]. Vyatta software along with the protocols, such as dynamic host configuration protocol (DHCP), network address translation (NAT), domain name server (DNS) and secure shell (SSH), are configured on a virtual machine workstation [3]. Drivers for Wi-Fi are implemented on Vyatta using communication device class (CDC) / network control model (NCM) drivers. CDC/NCM driver is a generic device driver for Linux that creates a network interface on Vyatta. Netgear router and uniform resource locator (URL) filtering can block the hypertext transfer protocol (HTTP) traffic, but not the HTTPS traffic on Internet Explorer. For example, the website http://www.facebook.com is blocked by the URL filtering while the https://www.facebook.com cannot be blocked [3]. Also, the existing software routers cannot block the HTTPS traffic while using private browsing on internet explorer [6]. There is a need to block HTTPS websites to secure confidential data across the network.

The design and development of integrated Wi-Fi module with Vyatta software router are not difficult. It can be developed on a virtual machine workstation. Design of the Vyatta software router is based on the Vyatta configurations for the DHCP, DNS, NAT and SSH protocol [3]. The design of the Vyatta software router is shown in Figure 3 [3]. The system was implemented using the latest version of VyOS on an Intel platform with core i5 5th Generation processor, 512 MB of Random Access Memory (RAM) and 2 GB of storage [3].

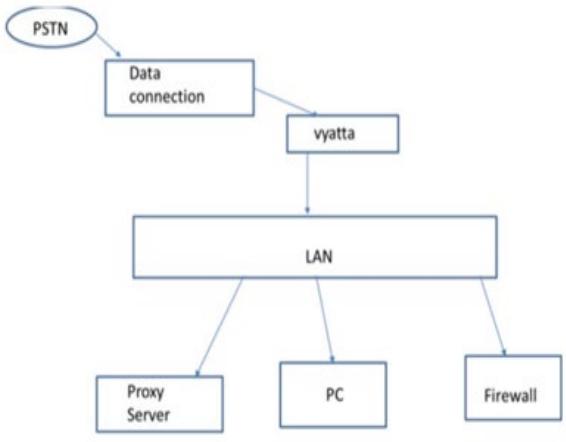

Figure 3. Design of Software Router Vyatta [3].

Figure 1 shows the Vyatta software router implemented between data connection and local area network (LAN) [3]. Public switched telephone network (PSTN) provides a data connection to the routers, which is Vyatta software router in this case. There are three different devices, a firewall, a personal computer (PC), and a proxy server, on LAN. All these three devices are integrated with Vyatta and configured. The management of these three devices is software based and hence they can be modified according to the requirement. In Vyatta software router, all the protocols such as DHCP, NAT, SSH and DNS are configured, along with the firewall policies [3]. Vyatta is implemented using image-based installation method. It does not alter files while booting the operating system. Each Vyatta release is self-contained within a directory on the selected storage device. It allows multiple images to be

installed on the same system, such as firewall, providing a predictable environment upon boot, and allows for a quick upgrade to a new release of Vyatta software router [3].

The result of testing of the developed and implemented Vyatta software router was successful. The testing is carried out on the integrated Wi-Fi module with Vyatta on Debian Jessie, with the aid of test cases developed [3]. The obtained test outcomes were studied and compared with the expected results. The Wi-Fi module drivers were implemented successfully [3]. Denying access using keywords and block category were shown in the test. The websites are successfully blocked and the connectivity to the websites is tested before and after enabling the block code on Vyatta [3].

In conclusion, integration of Wi-Fi module with Vyatta software router was carried out successfully. The security of Vyatta is enhanced, on both wired and wireless networks, by enabling the feature of blocking websites based on keywords. It reduces the cost since it is an open source system software router. Multiple websites can be blocked simultaneously, and hence it is scalable. From the test cases and the results, it is evident that the developed Vyatta software router performs better than the other hardware routers. Allowing users to change the required firewall policies and block the websites can lead to better results.

In **2018**, a paper on How Wireless Routers Can Jeopardize Your Secrets was introduced. In this paper, their major contributions were:

- They reported the timing side channel inherent in all generations of IEEE 802.11 or Wi-Fi technology. They show the timing channel is reliable and amplifiable.
- They showed that the side channel affects macOS, Windows, and Linux by studying the overlaps and differences in their TCP stack implementations.
- They provided a thorough analysis and evaluation of the proposed attack under different router/network/OS/browser combinations

The main concept behind this exploiting the timing channel was: The attacker sends a spoofed probing packet, along with a pre-probe query and post probe query to measure the RTT before and after; If the spoofed packet does not trigger an ACK on the client, because the guessed sequence number is in-window, then the post-probe query arrives at the client faster and gets back sooner; On the other hand, if the spoofed packet triggers an ACK on the client, e.g., because the guessed sequence number is out-of-window, then the post probe query experiences contention with the ACK from the client, and therefore prolongs the measured RTT.

Future work and research:

- Even though IEEE 802.11ax working group has been considering the possibility of supporting in-band full-duplex communication, research still needs to be done to make sure the real-world challenges such as backward compatibility is carefully considered and addressed.
- Manufacturers have begun introducing changes with features like embedded security, password policies, CAPTCHAs, and users' access control lists (ACLs), among others. These features, however, also mean additional costs for home users and thus become a big challenge for ISPs. As such, we believe that home routers will still be a prime target of cybercriminals.
- Why not all websites are encrypted, so that, the attacker cannot inject a malicious payload into the connection. All websites must run under the secure connection of HTTPS.
- The WPA3 seems to be the new cutting-edge technology, It promises to make the public network more secure and shall protect against brute force password attacks. This protocol is still in making but has already garnered a lot of attention from the techno world.

References:

[1]Park K., Yong Soo Kim Y., Kim J., (2012). Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router, 2012 14th International Conference on Advanced Communication Technology (ICACT), pp. 550-553, 2012.

[2]Waichal S., Sonune G., and Meshram B.B., (2013) June. Router attacks detection through log analysis and defense mechanism. IRACST – International Journal of Computer Networks and Wireless Communications (Vol.3, pp. 251-256).

[3] Chaitra S. and Sharma R., (2017). Integration of Software Router with Wi-Fi for Enhanced Security. 2017 IEEE 7th International Advance Computing Conference (pp. 33-36).

[4] Deb, S.S. and Munro, A., (2007) October. Closing the Loop for Dynamic IP QoS Provisioning: A Case Study. In Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on (pp. 368-375). IEEE.

[5] Digikey.com, (2011). Security Issues with WiFi Bluetooth and ZigBeeDigiKey

[6] Liu, A.X. and Gouda, M.G., (2008). Diverse firewall design. Parallel and Distributed Systems, IEEE Transactions on, 19(9), pp.1237-1251.

[7] Owning Your Home Network: Router Security Revisited.

[8] A Scalable Method for Router Attack Detection [2395]

[9] Release the Kraken New KRACKs in the 80211 Standard [2399]

[10] Weiteng Chen and Zhiyun Qian, University of California, Riverside, 2016, Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets, 27th USENIX Security Symposium.

[11] K. H. YEUNG and W. K. FUNG Attacking Routers by Packet Misrouting, 2004 Tele traffics and Networking Laboratory, City University of Hong Kong

[12] Joey Costoya, Ryan Flores, Lion Gu, 2016, Home Routers - Understanding Attacks and Defense Strategies, Trend Micro Forward-Looking Threat Research (FTR) Team, Trend Labs research paper.

[13] Saili Waichal, B.B.Meshram, Router Attacks-Detection And Defense Mechanisms, international journal of scientific & technology research volume 2, issue 6, June 2013