Plagiarism Checker X Originality Report

Similarity Found: 8%

Date: Tuesday, June 29, 2021
Statistics: 353 words Plagiarized / 4485 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

See discussions, st ats, and author pr ofiles f or this public ation at : https://www .r ese ar chg at e.ne t /public ation/322685383 QoS AND SECURITY OPTIMIZATION ON WIRELESS INFRASTRUCTURE NETWORK TOPOLOGY FOR WEB CONFERENCE SERVICE Article in F ar East Journal of Electr onics and Communic ations · Januar y 2018 DOI: 10.17654/EC018010113 CIT A TIONS 0 READS 321 2 author s , including: Some o f the author s o f this public ation ar e also w orking on these r elat ed pr ojects: F er dy Nir w ansy ah V ie w pr oject V essel Anomaly Behavior V ie w pr oject Suhar jit o Suhar jit o Bina Nusant ar a Univ er sity , Jak art a, Indonesia 124 PUBLICA TIONS 366 CIT A TIONS SEE PROFILE All c ont ent f ollo wing this p ag e w as uplo aded b y Suhar jit o Suhar jit o on 21 April 2018.

The user has r equest ed enhanc ement of the do wnlo aded file. Far East Journal of Electronics and Communications © 2018 Pushpa Publishing House, Allahabad, India http://www.pphmj.com http://dx.doi.org/10.17654/EC018010113 Volume 18, Number 1, 2018, Pages 113-131 ISSN: 0973-7006 Received: August 3, 2017; Revised: September 10, 2017; Accepted: September 20, 2017 Keywords and phrases: Wi-Fi, RADIUS, ARP, QoS, web conference, CVSS.

QoS AND SECURITY OPTIMIZATION ON WIRELESS INFRASTRUCTURE NETWORK TOPOLOGY FOR WEB CONFERENCE SERVICE Suharjito and Bayu Tapa Brata Department of Computer Science Binus Graduate Program Bina Nusantara University Jakarta, Indonesia e-mail: suharjito@binus.edu vincentbayu@yahoo.com Abstract When consumer-class Wi-Fi router's transfer rate becomes higher, many types of real-time multimedia communication services, such as web conference and unified communication (UC) can be run in middle and low-class business offices.

However, a real-time multimedia communication service should also be safe, both in the upper layer (application) and lower layer (data link). This work attempted to create balance optimization between QoS and security. Series of network stress test experiments with Jperf and penetration test with Kali Linux distribution were performed against three of wireless infrastructure topologies.

Typically for topology 1, experiments were carried out against 3 of Wi-Fi authentication standards (Open Security, WEP, WPA2 Personal TKIP and WPA2 Personal AES). QoS values (delay and packet loss) were recorded into tables and charts, while security vulnerabilities were recorded into CVSS (common vulnerability scoring system) framework.

Wi-Fi authentication standard with best QoS values and CVSS score was chosen to represent at topology 1 and Suharjito and Bayu Tapa Brata 114 compared against other topologies. Before topology 2 was examined, QoS optimization was performed for authentication and location was moved from wireless router into external RADIUS server. This server changed Wi-Fi authentication method from passphrase checking to public and private certificates/keys validation.

Optimization performed by QoS utility installation on OpenWRT firmware prioritized UDP and RTP traffics on Jperf's and VoIP server's ports. Another optimization treatment was performed by USB flash disk mounting to add extra swap/cache memory for OpenWRT system. Moreover, transmission frequency was changed from 20MHz to 40MHz On topology 3, optimization was performed by shortening route between wireless router and RADIUS server, namely radius utility installation as internal RADIUS server, on OpenWRT firmware.

Security hardening was performed by deploying ZRTP encryption and SRTP protocol into Android smartphone clients. Total QoS values and CVSS scores comparison proved that topology 3 is the best system for supporting multimedia real-time communication services like VoIP/UC. Topology 3's performance will be better when deployed into wireless router that has greater processor clock and more memory capacity. 1.

Introduction By 2018, it has been predicted that video conference will be the most used business communication method (Cisco [7]). Mobile devices owned by business professionals will dominate the real-time multimedia communication service. Internet data tr affic will consist of 65% video data transferred by mobile computer and portable communication devices. Figure 1.

Growth of global business communication services adoption (Cisco [7]). QoS and

Security Optimization on Wireless Infrastructure … 115 Substantively, many enterprise-class institutions in Indonesia still prefer to use WPA2 Personal for their daily operational Wi-Fi services rather than WPA2 Enterprise (with RADIUS server), although there are many proprietary RADIUS solutions with free and open source solution such as FreeRADIUS and OpenRADIUS.

Real-time communication is prone to eavesdropping risks, because of the nature of Wi-Fi router's ARP that is connectionless and stateless, thus it contains security holes (Ndueso et al. [16]). Compared to WPA2 Personal, WPA2 Enterprise involves more complex authentication process, but we will show that it would not give any significant bad effects compared to QoS (delay and packet loss) when they use AES as the cipher.

Security routines, router's processor power, and QoS have dependent relationship that work toward low-end, mid-end, high-end class Wi-Fi routers, as stated by Kofler et al. [11]. Maximum throughput of 270Mbps is attained by bypassingsecurity routines mid-end Wi-Fi router (TP-Link TLWR with OpenWRT firmware). Figure 2. Throughput vs packet size with/without security routines (Kofler et al. [11]). Another paper by Radmand et al.

[21] showed that security is a must for modern multimedia communication. However, security utilities like firewall Suharjito and Bayu Tapa Brata 116 and encryption algorithms (DES, 3DES, BlowFish, AES, RC2) caused delay and packet loss significantly. Their research used wired network and symmetric encryption as experimental base. Real-time multimedia communication needs low delay and packet loss.

As (ITU-T) [1] has already specified, maximum delay tolerance for real-time communication is 1 millisecond, as stated by Novella and Castano [18] whereas Kazemitabar et al. [10] described ideal packet loss threshold at 1-3% for two-way real-time communication. Various improvements were made by the developers of real-time- multimedia communication applications , one of which is Adobe's RTMP protocol that serves as an alternativ e to a more practical use with web browser plug-in (Flash Player).

It is flexible to gateway server's NAT configurations and adaptive to network conditions compared to SIP protocol (main protocol in the unified communication) (Selvapriya et al. [23]). As Yuan [28] explained, session initiation protocol (SIP) that is the basis of VoIP and unified communication's main service performs audio/video codec negotiation only once and it is used throughout the communication sessions, so that it ignores changes on the network condition that frequently occurs on wireless network.

Figure 3. SIP stack (Yuan [28]). Audio/video codec renegotiation process through REINVITE message sending proposed by Aktas et al. [2] was created to overcome SIP QoS and Security Optimization on Wireless Infrastructure ... 117 disadvantage, however, it is not practical and efficient as client's device is forced to do redial. Figure 4. VoIP codec renegotiation process (Aktas et al. [2]).

Another typical problem in SIP implementation as real-time multimedia communication basis is firewall's NAT traversal. Generally, firewall policy blocks services that open to many ports that increase security risks (port vulnerability manipulation). SIP's respond message on UDP packet sent with RTP was identified by Yeryomin et al. [27] as the source of problem because it needs to open port UDP 10001-20000.

Other than that, SIP INVITE messages need to open port UDP 5060-5061. Figure 5. SIP problem on firewall's NAT traversal (Yeryomin et al. [27]). Suharjito and Bayu Tapa Brata 118 For the reason of security risks, another real-time multimedia communication protocol was used in this case study. Adobe's RTMP seems to be a more flexible alternative. Si milar to SIP, RTMP uses UDP but it can easily pass firewall's common NAT policies.

Web conference using RTMP needs only web browser plug-in, so that it can run on PC, laptop, tablet PC, and smartphone. It also works across operating system platforms. Although RTMP is not an open source platform, but it is free to use, therefore it can be used and deployed by small business. One of the proofs that RTMP is sufficiently reliable to handle critical mission is a case study performed by Santos et al. [22].

In their work, RTMP was used to serve collaboration research on atom fusion between Lisboa Nuclear Reactor Laboratory and Madrid Nuclear Reactor Laboratory. The optimization of security and quality of services (QoS) guarantee in wireless sensor networks was proposed using ad-hoc on-demand distance vector (AODV) protocol called QwS-AODV protocol . This protocol can add or remove security services dynamically according to the network performance (Rachedi and Hasnaoui [20]).

A study of QoS-adaptive service configuration model has been done by Alamri et al. [3] in a cloud-assisted video surveillance prototype to explain a video processing requirements in terms of bandwidth, delay, and frame rates. 2. Literature Review When two computer devices can interconnect and communicate or exchange information and share resources, the first and simplest network mode formed is a two-way peer to peer (PTP) or ad-hoc, which resembles an open curve. The topology form that exists in the mode of PTP other than line topology is a ring topology.

This topology is one-way and it resembles a closed curve. The development of the number of nodes (connected devices) leads to the need for a central conn ection device (server) as well as a central link (backbone line). Thus, star topology and bus topology were formed.

The variation of the two topologies, the mesh topology, is present to provide redundancy to malfunctions in both the central line and the central device QoS and Security Optimization on Wireless Infrastructure ... 119 (Xian and Huang [26]). The idea of a central switching device leads to the second mode of infrastructure. If these two network modes are compared for VoIP service research, then infrastructure mode is more relevant (Al-Kharobi and Al-Mehdhar [4]).

According to Singh and Jain [24], ad-hoc or PTP mode requires enormous resources to maintain and manage the complexity of routing that changes frequently due to the movement of other nodes. In addition, each node in PTP mode has its own algorithm that is different in time synchronization, power management, packet scheduling, and others.

All these factors can reduce QoS performance and network security. Associated with the local network topology using VoIP service as a form of real-time communication, this research will use the basic form of star topology. This is based on a research by Buettrich and Pascual [5] which states star topology as a standard form of wireless network, especially if the network mode used is infrastructure.

Some user authentication methods in infrastructure mode have been comm only used, for example authentication with WEP (wired equivalent privacy) encryption, WPA (Wi-Fi protected access), and WPA2 Personal. The principle of the authentication system is by granting access permission as far as knowing the password. In its development, authentication with WEP encryption was successfully solved in just a few minutes.

Meanwhile, authen tication security with WPA2 Personal encryption is highly dependent on p assphrase power and vulnerable to ARP positioning attacks. User authentication vulnerability problems in infrastructure network mode can be solved by adding RADIUS server (remote authentication dial in user service) in network topology. This server contains the user database, username, password, and au thentication certificates of each user.

Prior to granting access, authentication with WPA2 Enterprise will validate usernames, passwords, certificates / private keys, and public key certificates to the RADIUS server. If validation succeeds, then access is granted. The position of the RADIUS server in the

third topology of this research experiment will be changed by installing it into the wireless router, assuming it will shorten the routing and speed up the user authentication process.

In Suharjito and Bayu Tapa Brata 120 this implementation, there are several common topologies in small-scale local office networks that use unified communication (Persky [19]). In this topology, unified communication servers are not located within the local network, but on the Internet because these types of offices generally use cloud-based real-time communication services, such as Skype. Other topologies also support unified communication services, but they are local server-based (Chakraborty et al.

[6]). The server functions to authenticate registered service users and control the communication session. In this topology, other than unified communication service server, there were additions, i.e., user device in the form of smartphone and a wireless router that connects between users in local network.

Before accessing the unified communications service, the wireless connection user must authenticate using WPA2 Enterprise where the user, password and certificate / private or public key installed on the user's device are compared to the database in the RADIUS server. In its development, current communication that is real-time and involves multimedia content started to be performed over the wireless network because of the performance of fast growing wireless router. Past researches by Kofler et al. [11] suggested that wireless routers that use medium and processor memory, such as the 802.11n standard, are capable of supporting services involving multimedia data with a maximum throughput performance of 270Mbps.

Their experiment was performed using the data packet size 1450 Byte or known as jumbo frame. However, this study did not measure the achievement of delay and packet loss values that are sensitive to real-time and multimedia communication performance, such as VoIP.

In addition, the research did not involve user authentication such as WEP, WPA2 Personal, or WPA2 Enterprise, so it did not display the security effect on network QoS (Mohammed and Ali [13]). The discussion on real-time transport protocol (RTP) was important in this research because almost all features of unified communication service use RTP protocol.

All new multimedia communication systems are run with a network protocol base called RTP. The development of the RTP protocol is QoS and Security Optimization on Wireless Infrastructure … 121 under the coordination of the agency's audio-video transport

working group, as a part of the Internet engineering task force (IETF). The RTP specification is set up in the request for comments (RFC) 1889 and RFC 3550 documents.

RTP is a primary protocol that delivers streams of audio-video data between users, but it is not a single protocol. RTP is run in conjunction with the real- time transport control protocol (RTCP), a compliant protocol that controls the statistics and QoS of the audio-video data stream transmission and helps manage the synchronization of multiple data streams (Durresi and Jain [8]).

Secure real-time control protocol (SRTP) provides safe audio-video payload through encryption, authentication, and data integrity. Encryption is carried out with AES cipher and single m aster key. A protocol is required to set up the exchange of a single master key, for instance Zimmerman RTP (ZRTP) and multimedia Internet keying (MIKEY).

Authentication of the audio-video payload on SRTP is performed to test the integrity of the information through the checksum process using HMAC-SHA1 algorithm, which yields 160 bits (Fernandez et al . [9]). Audio-video payload encryption was performed in this study using the ZRTP master key protocol so that the client's mobile communication device could perform master key derivative exchanges with the VoIP service server (M ueed et al. [14]).

The application of encryption to audio-video payloa d was assumed to degrade QoS network connection performance. Thus, this study compensated by shortening the routing between RADIUS servers and wireless routers. The security of information systems is an attempt to retain information from unauthorized access, use, disruption or harassment, alteration, recording and destruction.

Information system security, abbreviated with InfoSec, measures three elements, namely: availability, confidentiality and integrity (Mawale et al. [12]. The measurement of information system security is qualitative, so it requires a special way to be quantified, for example by processing it using the common vulnerability scoring system or abbreviated CVSS (Tripathi and Singh [25]).

Based on the CVSS implementation guide document (National Institute of Sta ndards and Technology-NIST [15]), the Suharjito and Bayu Tapa Brata 122 CVSS security assessment is divided into three areas: base metrics, temporal metrics and environmental metrics. The final value of the CVSS is the accumulation of the values in each measuring region. The values of 0-3.9 are categorized as low, 4-6.9 moderate, and 7-10 high.

Higher the value, greater is the security risk and the potential losses. 3. Methods There were three variations of Wi-Fi infrastructure topologies that were proposed and accessed with two different methods, namely network stress test and security penetration test.

The first method was performed with flash video stress test tool called Flazr installed on accessor's laptop while the second method was performed with sev eral Kali Linux's utilities, such as airodump-ng, aireplay-ng, aircrack-ng, ettercap and Wireshark. All of these security assessment tools are bundled on Kali Linux distribution. Figure 6. Kali Linux.

The first and third topologies proposed on this research were based on the results of a study performed by Buettrich and Pascual [5] on star topology that was used as basic Wi-Fi forma tion on infrastructure mode, whereas the second topology was based on the research carried out by (Asra and Pasha [5]) who tested combination between star and bus formation called hybrid topology.

QoS and Security Optimization on Wireless Infrastructure … 123 Forth stress test, Wireshark installed on accessor's laptop captured video stream packet that was sent by Re d5-MediaServer and recorded the QoS values (delay and packet loss). This t est was repeated with increasing packet amount with the interval of 5MB/s, started from 5MB/s to 30MB/s.

This set of tests was repeated for 5 times to achieve consistent result. High level security assessment was performed on WPA2 authentication system. Aireplay-ng was used to force the client's laptop to reconnect to wireless router. While the client's laptop was sending authentication packet containing passphrase key, the second Wi-Fi adapter on accessor's laptop captured those packets with airodump-ng utility. Finally, captured packets were cracked with airocrack-ng to reveal passphrase key. Low level security assessment was performed to test ARP vulnerability.

Ettercap utility was used to do ARP poisoning attack and takeover Wi-Fi router's role as a central node. Traffic of all packets that passed through accessor's laptop was captured and decoded by Wireshark utility, including RTMP and UDP, which contained video or audio packets.

Penetration test was performed as a "proof of concept" for existence of vulnerabilities on each of Wi-Fi authentication security (WPA2 Personal and WPA2 Enterprise). Number of vulnerab ilities and risk level were converted from qualitative to quantitative values with CVSS (common vulnerability scoring system) framework. This score w as taken to

be compared with the second and third topologies. Figure 7. First network topology.

Suharjito and Bayu Tapa Brata 124 Instead of WPA2 Personal, the second topology used WPA2 Enterprise with RADIUS server as an authentication method. We used Zeroshell Linux distribution as RADIUS server, other than wireless router. We wanted to observe WPA2-cracking effectivity against WPA2 Enterprise. Besides that, we also wanted to prove ARP attack effectivity against the Wi-Fi router's original firmware on low level security. Figure 8. Second network topology.

This research was conducted with TP-Link TL-WR1043ND. This wireless router represents middle class processor power, memory capability, and transfer rate used often by small offices. On the third topology, standard firmware from TP-Link was replaced with Linux based firmware: OpenWRT. Figure 9. Third network topology.

QoS and Security Optimization on Wireless Infrastructure … 125 Internal RADIUS server was applied through radius utility so that it was possible to add low level security strengthening. ARP table utility and custom policy were added into this firmware to prevent ARP poisoning attack. Figure 10. ARP security hardening (Tripathi and Singh [25]).

CVSS platform and metrics usage were adopted from the research performed by Tripathi and Singh [25] that depicted trends of general security threads and took data from United States National Vulnerability Database. Suharjito and Bayu Tapa Brata 126 Figure 11. CVSS V.2 calculator (NIST [17]). 4. Results and Discussion Packet delay comparison graph shows that the third topology generates shortest delay timer, although it is slightly different with the second topology. It proves that the distance between RADIUS Field Code Changed server and Wi-Fi router has no significant impact to packet delay time.

More complex authentication method in WPA2 Enterprise did not generate significant additional delay effect, compared to simpler authentication in WPA2 Personal, as long as they use similar cipher. QoS and Security Optimization on Wireless Infrastructure … 127 Figure 12. Delay comparison. In terms of packet loss, second topology gave the best result. It had packet loss value less than 1%.

Flash memory space consumption for several utilities (radiusd and ARP tables) on Wi-Fi router generated significant negative effect to packet loss in the third topology. Figure 13. Packet loss comparison. From the security perspective, topology 3 showed the highest security level. It was obtained from combination between internal RADIUS server (radiusd utility on OpenWRT firmware), ARP security protection (with ARP tables utility),

and custom ARP rule that kept the validity to central node's IP-MAC address pairing.

Suharjito and Bayu Tapa Brata 128 WPA2 cracking attack was successfully performed on the first topology, but it was not successful on the second and third topologies. It was caused by failure on forcing client to do re_a uthentication so that there was no authentication packet containing passphrase key to be captured and decoded. Meanwhile, custom ARP tables rule gave extra protection to low level security (ARP vulnerability) against ARP poisoning attack.

Packet eavesdropping and decoding cannot be pe rformed if ARP poisoning failed. This system worked well on the third topology. Figure 14. CVSS V.2 score comparison. 5. Conclusion The third Wi-Fi topology performed the highest values on security, but the second topology generated best values for QoS. The third topology achieved shorter packet delay when it was deployed on Wi-Fi router with higher flash memory capacity and processor power that was sufficient to handle security utilities workload. The Wi-Fi 802.11N standard provided the most ideal support for multimedia real-time communication services such as VoIP / UC on the use of 1000-1400 Byte data packet fragmentation sizes. This finding could be achieved with the use of audio / video codec that gave the best result on bitrate 1000-1400 bytes per second.

Payload of encrypted QoS and Security Optimization on Wireless Infrastructure … 129 packets in this study used ZRTP and RTP transport protocols, which were also encrypted by using SRTP, was ab le to strengthen confidentiality and integrity in real-time communication with VoIP. Further research can be done to compare performance of alternative wireless router firmware, such as DD-WRT, Tomato and Gargoyle.

Research on the influence of antenna type and signal modulation method is hi ghly potential in affecting the performance of wireless network QoS. Furthermore, the influence of the number of hop or bridging factor (point to point) on QoS and security needs to be studied and optimized. Acknowledgement The authors thank the anonymous referees for their valuable suggestions for the improvement of the manuscript.

References [1] International Telecommunication Unit (ITU), Quality of Service and Dependability Vocabulary, Fascicle II.3 Rec. E.800, 2007, pp. 1-16. [2] I. Aktas, F. Scmidt, E. Weingartner, C. J. Schnelke and K. Wehrle, An Adaptive Codec Switching Scheme for SIP-based VoIP, Springer-Verlag, 2012. [3] A. Alamri, S. M. Hossain, A. Almogren, M. M. Hassan, K. Alnafjan, M. Zakariah and A.

Alghamdi, QoS-adaptive service configuration framework for cloud- assisted video

surveillance systems, Multimedia Tools and Applications 75(21) (2016), 13333-13348. [4] T. Al-Kharobi and M. A. Al-Mehdha r, Comprehensive comparison of VoIP SIP protocol problems and Cisco VoIP system, International Journal of Network Security and its Applications (IJNSA), (2012), 137.

[5] Anjum Asra and Shaik Apsar Pasha, A brief view of computer network topology for data communication and networking, International Journal of Engineering Trends and Technology 22(7) (2015), 319-324. Available from: http://www.ijettjournal.org. [6] T. Chakraborty, A. Mukhopadhyay, S. Bhuni a, S. I. Misra and K. S. Sanyal, An optimization technique for improved VoIP, Journal of Networks 7(3) (2012), 484. [7] Cisco, Cisco 2014 Midyear Security Report, 2014.

Suharjito and Bayu Tapa Brata 130 [8] A. Durresi and R. Jain, RTP, RTCP, and RTSP-Internet Protocols for Real Time Multimedia Communication, The Industrial Information Technology Handbook, CRC Press, 2005. [9] E. B. Fernandez, J. C. Pelaez and M. M.

Larrondo-Petrie, Security patterns for voice over IP networks security patterns for voice over IP Networks, Journal of Software V (2007), 19-29. [10] H. Kazemitabar, S. Ahmed, K. Nisa r, A. B. Said and H. B. Hasbullah, A comprehensive review on VoIP over wireless, International Journal of Computer Science Letters 2(2) (2010), 1-16. [11] I. Kofler, R. Kuschnig and H.

Hellwagner, Evaluating the Networking Performance of Linux-based Home Router Platforms for Multimedia Services, Institute of Information Technology, Alpen-Adria-Universitat, Austria, 2011. [12] R. K. Mawale, M. D. Dakhane and L. R. Pardhi, Authentication methods for Wi-Fi networks, International Journal of Application or Innovation in Engineering and Management (IJAIEM) 2(3) (2013), 356-360.

[13] A. H. Mohammed and H. A. Ali, Eff ect of some security mechanisms on the Qos VoIP application using OPNET, International Journal of Current Engineering and Technology 3(5) (2013), 1626-1630. [14] S. A. Mueed, M. Salman, R. Ali and S.

Ghafir, Android driven security in SIP based VoIP systems using ZRTP on GPRS network, IRACST - International Journal of Computer Networks and Wireless Communications 2(2) (2012), 209-217. [15] National Institute of Standards and Technology-NIST, CVSS Implementation Guide, NISTIR 7946, 2014. [16] J. S. Ndueso, C. Ndujuiba and U. A.

Nwamara, Developed secure network model using RADIUS server, International Journal of Engineering Science and Innovative Technology (IJESIT) 2(2) (2012), 1-6. [17] NIST,

Computer Security Resource Center - National Vulnerability Database, Retrieved from Common Vulnerability Scoring System Calculator Version 2, 2016. https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator. [18] I. M. Novella and F. J. Castano, QoS Requirements for Multimedia Services, Resource Management in Satellite Networks, 2007, pp. 67-94. [19] D.

Persky, VoIP Security Vulnerabilities, SANS Institute Info Sec Reading Room, SANS Institute, 2007. QoS and Security Optimization on Wireless Infrastructure ... 131 [20] A. Rachedi and A. Hasnaoui, Advanced quality of services with security integration in wireless sensor networks, Wireless Communications and Mobile Computing, 2015, pp. 1106-1116.

[21] P. Radmand, J. Singh, M. Domingo, J. Arnedo and A. Talevski, The Impact of Security on VoIP Call Quality, 2011. [22] S. Santos, R. Castro, J. Santos, D. Gomes, H. Fernandes, J. Sousa and C. Varandas, Open Meetings as a Br owser-based Teleconferencing Tool for EFDA Laboratories, Elsevier, 2011. [23] P. Selvapriya, K. Maheswari, and V.

Hemala tha, Performance issues in mobile ad hoc, International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE) 3(2) (2015), 1033-1038. [24] R. K. Singh and A. Jain, Research issues in wireless networks, International Journal of Advanced Research in Comput er Science and Software Engineering, (2012), 115. [25] A.

Tripathi and K. U. Singh, Analyz ing trends in vulnerability classes across CVSS metrics, International Journal of Computer Applications 36(3) (2011), 38. [26] Y. Xian and C. T. Huang, Securing VoIP Services in Multi-Hop Wireless Mesh Networks, IEEE Explore, 2007. [27] Y. Yeryomin, F. Evers and J. Seit z, Solving the Firewall and NAT Traversal Issues for SIP-based VoIP, IEEE Explore, 2008. [28] Z.

Yuan, SIP-based VoIP Network and its interworking with the PSTN, Electronics and Communication Engineering Journal, Faculty of Information Engineering and Technology, Shandong University, 2002. View publication stats View publication stats

INTERNET SOURCES:

---

e-quality-of-the-solution-for-the-multiperiod-installation-problem-using-modified-prim-s-algorithm.html
<1% - https://www.academia.edu/9833111/ANALYSIS_AND_DESIGN_OF_AGRICULTURAL_INSURANCE_DATABASE_SYSTEMS_AND_MAPPING_AGRICULTURAL_INSURANCE_WEB_BASED
<1% - https://linux-archive.web.cern.ch/scientific6/docs/rhel/6.1_Technical_Notes/
<1% - https://www.cloudradius.com/is-there-a-freeradius-gui/
<1% - https://downloads.hindawi.com/journals/scn/2020/5429630.xml
<1% - https://b-ok.org/book/2080266/abe31f
<1% - https://www.atlantis-press.com/article/25848184.pdf
<1% - https://neptune.ai/blog/machine-learning-model-management
<1% - https://dl.acm.org/doi/abs/10.1002/wcm.2562
<1% - https://link.springer.com/article/10.1007%2Fs11042-015-3074-7
<1% - http://www.journaltocs.ac.uk/index.php?action=tocs&journalISSN=1053-587X
<1% - https://www.mdpi.com/2078-2489/8/3/76/htm
<1% - https://quizlet.com/469603319/security-practice-questions-flash-cards/
<1% - https://journals.sagepub.com/doi/full/10.1155/2014/532043
<1% - https://www.vskills.in/certification/tutorial/tcp-ip-protocols-and-ports/
<1% - https://iaoc.ietf.org/documents/morris-signed-Sony-v-SSH_000.pdf
<1% - https://tools.ietf.org/id/draft-ietf-rtcweb-rtp-usage-04.html
<1% - https://tex2e.github.io/rfc-translater/html/rfc5197.html
<1% - https://hpbn.co/webrtc/
<1% - https://dokumen.pub/engineering-information-security-the-application-of-systems-engineering-concepts-to-achieve-information-assurance-1nbsped-0470565128-978-0-470-56512-4-978-0-470-94791-3-978-0-470-94783-8-978-1-118-00901-7.html
<1% - https://www.ocio.usda.gov/sites/default/files/docs/2012/DM3540-001.htm
<1% - https://linuxbsdos.com/2015/10/24/how-to-triple-boot-ubuntu-15-10-kali-linux-2-windows-10-on-a-pc-with-uefi-firmware/
<1% - https://quizlet.com/96118085/ceh-flash-cards/
<1% - https://dokumen.pub/comptia-cybersecurity-analyst-cysa-cs0-002-cert-guide-2nd-edition-certification-guide-2nbsped-9780136747161.html
<1% - https://unix.stackexchange.com/questions/76324/tp-link-tl-wr1043nd-as-dumb-access-point
<1% - https://www.routersecurity.org/resources.php
<1% - https://www.emerald.com/insight/content/doi/10.1108/S1479-359820160000006002/ful

l/html
<1% - https://dl.acm.org/doi/10.1145/3312574
<1% - https://ijnsa632102087.wordpress.com/2019/10/
<1% - https://ijettjournal.org/archive/ijett-v22p267
<1% - https://dblp.org/db/books/collections/IITHandbook2005
<1% - http://public.eng.fau.edu/ceecs/zhuang/EdFernandezCVApril25-11.doc
<1% - https://dblp.uni-trier.de/db/journals/jsw/jsw2
<1% - http://www-itec.uni-klu.ac.at/bib/files/platformeval_preprint.pdf
<1% -
https://studylib.net/doc/18754074/untitled---international-journal-of-engineering-and-advanced
<1% - http://eprints.covenantuniversity.edu.ng/view/subjects/TK.html
<1% - https://csrc.nist.gov/
<1% - https://link.springer.com/article/10.1007/s11277-021-08109-8
<1% - https://cv.archives-ouvertes.fr/abderrezak-rachedi
<1% - https://www.sciencedirect.com/science/article/pii/S0278612518303650
<1% -
https://www.academia.edu/25241031/Journal_of_Computer_Science_IJCSIS_March_2016_Part_I
<1% - https://ijcnc.com/2019/10/12/ijcnc-01-6/
<1% - http://gwep.usc.edu/wp-content/uploads/2020/10/Edited-TICS.pdf