International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Vulnerabilities of Intelligent Network System

Ahmed Refaat Ragab

Abstract: ***The intelligent network (IN), plays an important role in the telecommunication process, as a part of the human life. Although, the numbers of network vulnerabilities discovered each year are growing rapidly, and it becomes impossible for system administrators to keep the software running on their network machines free of security bugs. Thus, it is important to clear the vulnerability of certain network or system, this paper investigates the vulnerability analysis of intelligent network (IN), by giving a clear study of the vulnerability analysis of the intelligent network , by applying two scenarios, one is done using different types of operating systems trying to hack them and the other scenario by studying the routing vulnerability problems. This study can be valuable to another research and development work.***

Keywords: ACL, IN, SS7, UPT, VPN.

I. INTRODUCTION

Since 1950's IN system was used in telephone services, then in 1960's and because of the need for data transfer services the packet Switched data networks were developed especially for corporations use, and finally came the GSM (Global System for Mobile communications) mobile phone technology, which was introduced in 1991, to use low-speed data transfer.

The Intelligent Network (IN) can be defined as the capability to integrate all the telecommunications services mentioned in a flexible way, such as Freephone, Universal access number, Premium rate service, Credit or account card service, Universal personal telecommunication (UPT) and the Virtual private network (VPN) [1,2].

Regardless of the access medium and the coverage of a network, network security can be considered through the achievement of two security goals, computer system security and communication security.

And by focusing on the component of the vulnerabilities we found that it consists of the weakness equipment of the system or network, operating system, network structure and the protocols.

This paper experimentally investigates the vulnerability analysis of the intelligent network, the paper is organized as follows; section two discusses computer and network hacker exploits, section three reveals physical vulnerability, section four demonstrates network structure vulnerability, section five discusses software vulnerability, section six discusses application vulnerability, section seven experimentally examines the protocol vulnerability and finally section eight discuss and conclude the paper.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Ahmed Refaat Ragab*, Computer Science department, Faculty of Information Systems and Computer Science, October 6 University, Giza, Egypt. Email: ahmed.refaat.csis@o6u.edu.eg

II. COMPUTER AND NETWORK HACKER EXPLOITS

There is a vital need to know how hackers thinks to exploit a system, in order to give an efficient vulnerability analysis [4,5]. Hackers think in five main steps; reconnaissance, scanning, exploiting the System, keeping access and covering the tracks.

In reconnaissance, attacker conducts an open source investigation to gain information about the target, Scanning meaning the attacker uses a variety of mechanisms to survey the target and finding gaps in the target's defenses. Attacker exploit the system by trying to gain access or deny access to other users, then keeping Access, in which Attacker maintains access by manipulating the software installed on the system to achieve backdoor access.

Finally, the attacker covers his tracks by maintaining access while hiding from users and system administrator using a variety of mechanisms.

There are many tools that can be used by the hackers in each step, such as who is, Dns introgation, maltego, ip scan, super scan, port scanner, nmap, wire shark, john the riper, air crack, achillis, cain and abel, kismet and many other tools. Some of these tools will be used in this paper to evaluate the vulnerability problems.

III. PHYSICAL VUNERABILITY

Physical vulnerability of IN is mostly similar to any network as equipment damages. The damage to the equipment is mostly from, the natural disasters and man-made deregulation [6].

So, the protection is available to set in the ways of increasing devices, using standby systems, and deploying efficient scenarios, this yields in high costly solutions, but in the case of IN the data system is centralized, all the user's account and attribution information are stored in the data system center.

If the data system center crashes, no IN service can be served, so the protection of data system center should be enhanced. The common disk array storage and redundant database system have the ability to overcome hardware and software physical vulnerability problems [7].

Figure.1, shows a company's requirements, as the headquarters network must be protected from the external area, so that the best position for most sensitive servers is within the internal area and Because of its border position, the router is highly likely to be attacked from Internet, and with its Access Control List (ACL) configuration, only the most basic network attack attempts are blocked.

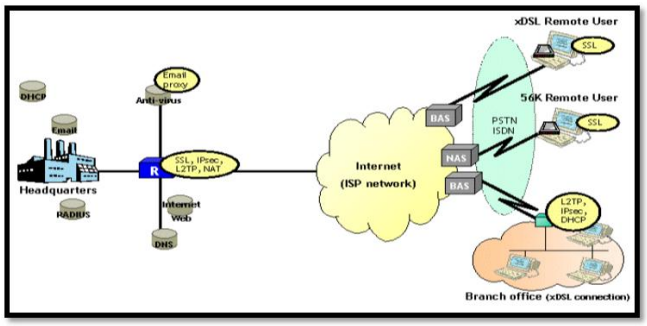

Fig. 1. A Company architecture with minimal protection [5].

IV. NETWORK STRUCTURE VULNERABILITY

The network structure of IN is the entry points that allow users to access and contribute to the overall system design, the communication between the main functional entities of the Service Control Point (SCP), Service Switch Point (SSP) and the Independent Peripheral (IP), is based upon the No.7 signaling transaction.

Although, the communication between the Service Management point (SMP) and the Service Control Point (SCP) depends on the Internet Protocol (IP), so the intrusion can come from the clients of SMP and infects the SCP [8].

Figure.2, shows the intelligent network structure, pointing at how Intelligence is provided and distributed in the network.

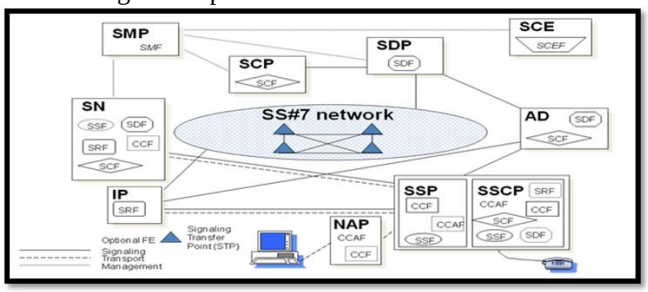

Fig. 2. Intelligent Network Structure [5].

Regardless of the access medium and the coverage of a network, network security can be considered through the achievement of two security goals, the computer system security and the communication security. The goal of computer system security is to protect data and information, assets against malicious or unauthorized use as well as to protect the data and information stored in computer systems from modification, destruction, or unauthorized disclosure [9,10].

While, the goal of communication security, is to protect information during its transmission through a communication medium from unauthorized disclosure, modification, or destruction [9,10].

V. SYSTEM SOFTWARE VULNERABILITY

IN system can be built on any universal Operating System platform, such as UNIX, Linux or Windows series (OS).

Generally, system software is OS and utilities, for any kind of software, the vulnerability is coming from the design and implementation of the code, most malicious software, such as Virus and Trojan horse has to get the administrator authorization to install or write data into system files.

Operating systems are huge and contain many bugs meaning errors in code, Linux contains for every 1,000 lines inside the code about 0.17 bug [12].

However, most commercial software contains for every 1,000 lines inside the code about 20-30 bugs, and the most recorded was windows operating system, which reported 81 bugs a day, and some of these bugs create vulnerabilities and they are the main source of these vulnerabilities [12].

Although, System software vulnerability is experimentally examined by proposing scenarios, using different operating system platforms, the proposed scenario uses virtual machines (sun virtual box), with two different operating systems, windows and Linux [12].

The scenario as shown in figure. 3, simulates a small office containing three systems victim1 and victim2, running windows operating system, while victim3 is running the Linux operating system and outside the small office there is a hacker pointing to exploit these systems, the hacker is using windows operating system and some hacker tools, such as network scanner, port scanner and air crack, figure. 4, shows the network scanner tool, which the hacker is using, showing the IP address for victum1, victum2, while victum3 was hard to discover, due to the authenticated software used presented as Linux. This experimental result proves by exploiting these two platforms, the fragility of windows software versus the robustness of Linux software.

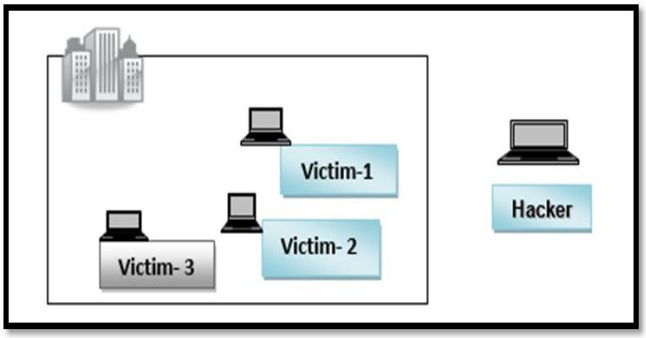

Fig. 3. A scenario for software attack.

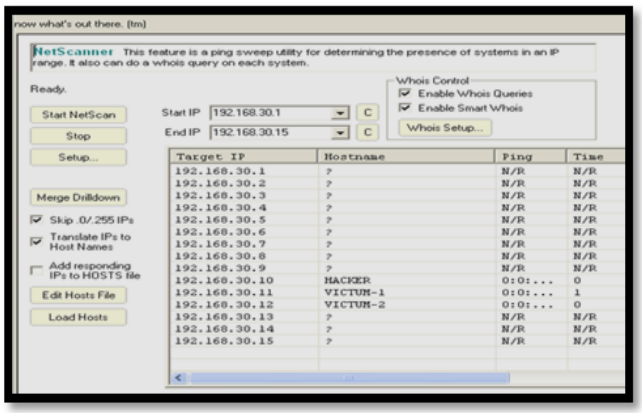

Fig. 4. Hacker network scanner tool.

VI. APPLICATION VULNERABILITY

The applications of IN are actually the different kinds of IN services, that can be provided.

Whereas, in the traditional telecom network, no risk is concerned for IN services, because all services are loaded, updated and removed by the operators [11].

Any useful application needs to be managed and administered, and this facility often forms a key part of the application security mechanism, providing a way for administrators to manage user accounts and roles [11].

The applications of the IN attract the attacker as the honey attracts the bees, as an example; the authentication mechanism weaknesses may enable an attacker to gain access as an administrator, which is the most powerful damage for the whole entire application.

Also, many applications do not implement effective access control of some of their administrative functions. An attacker may find a means of creating a new user account with powerful privileges.

VII. PROTOCOL VULNERABILITY

The protocol vulnerability is coming from the bearing signaling No.7, SS7 systems are networked using Internet technologies, and often the Internet itself.

Thus, SS7 vulnerabilities can affect the Internet, and also the internet vulnerabilities can affect SS7 networks [7].

Although, the Intelligent Network Application Part (INAP) is transmitted without encryption, it was found that the interception, eavesdropping and analysis of INAP is easy.

While, the authentication among signaling points is short, the availability of the network is affected directly.

Whereas, in a private closed network environment the authentication is unwanted, since the PSTN may be linked to the IP network and the number of operators, and the security of the network are subjected to threats [9].

It was found that without authentication and authorization among signaling points, the signaling systems can't control and avoid the malicious accesses, this will affect the network availability and reducing of operator control ability of the network, No.7 signaling is safer than TCP/IP protocol, but it also has some defect which can be discussed as causes of SS7 link problems:

A. Point code mismatch

The Originating Point Code (OPC), was defined in the ss7 as the stack configure message that matches the value of the distant end signaling point expects.

Also, the Adjacent Point Code (APC) and the Destination Point Code (DPC) values, must match the distant end's point code, which is clearly defined as a set configure message and SS7 signaling route configure message in the SS7 Signaling Link [7].

B. Signaling link code mismatch

The Signaling Link Code (SLC), which is assigned by both ends is identified as a number (0-15), to identify a specific link within a link set. It is clear that the SLC defined in the SS7 Signaling Link Configure message, must match the SLC value assigned to the link by the distant end [7].

C. Network indicator mismatch

The Network Indicator (NI) value is defined by two bits, therefore values 0-3 are possible, where the default value of the Network Indicator is set to National as 0x02 for both ANSI and ITU [7].

Whereas, some networks may require the Network Indicator to be set to International as 0x00 or one of the spare values as 0x01 or 0x03 [7].

D. Link status signaling unit size mismatch

By default, the MSPs transmit a Link Status Signaling Unit (LSSU), with a two-octet status field. Some signaling points may require an LSSU size of one octet, and in order to change the LSSU size, a PPL Configure Message needs to be sent to component MTP2 TXC [7].

E. Path and rate problem

A span carrying the signaling link must be configured for clear channel operation, in service, and not experiencing slips. Both parties must agree upon the time slots used to carry the signaling link.

Additionally, the data rate of the signaling link must be the same on both sides, and the Service State Configure message for signaling links is different than the Service State Configure message used for channels. The signaling link time slot and data rate are defined in the SS7 Signaling Link Configure message [7].

F. No route defined

A valid SS7 route must be defined for the destination to enable the MSP to send messages, and this is typically indicated by receiving Signaling Link Testing Message (SLTM) with no SLTMs being sent by the MSP [9].

Whereas, the vulnerabilities of MTP3 (signaling network), presents five aspects as follow; Clear text-based transmission, Routing problem, Lack of authentication and access control, Lack of the inspection for messages and No alarm and control of attacking [6, 9].

Routing vulnerability problem is examined in this paper, a proposed scenario shown in figure 5 is simulated by using Cisco packet tracer, the network architecture proposed in the scenario is being considered as a six connected nodes, after establishing and configuring the nodes, the topology was examined by sending packets, showing the routing table for node D.

Figure. 6, shows the routing table for node D, where all links are connected and up, and by Considering the same network architecture, but with a failure in the link between node C and node D, and it is clear in Figure. 7 showing the routing table for node D, when CD link is down.

Whereas, Figure.8, shows the routing table for the node D, when the links between C and D, A and D are down, and figure. 9, shows the routing table for the node D, when the links between C and D, A and D, the Link between B and D are down.

Also, figure. 10, shows the message sent between node D and C, where all the links are connected and the status is up, figure. 11, shows the message sent between nodes D and C, were the links between the nodes C and D are down, figure. 12, shows the message sent between nodes D and C, where the links between C and D, A and D are down, and finally figure. 13, shows the message sent between the nodes D and C, where the links between C and D, A and D and the nodes B and D are down.

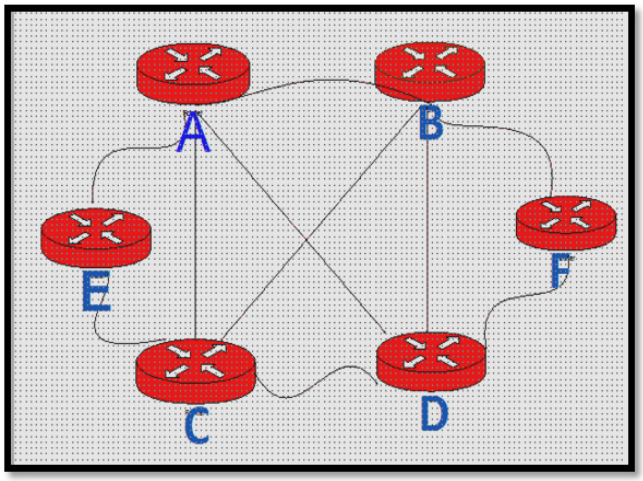

Fig. 5. Routing scenario topology.

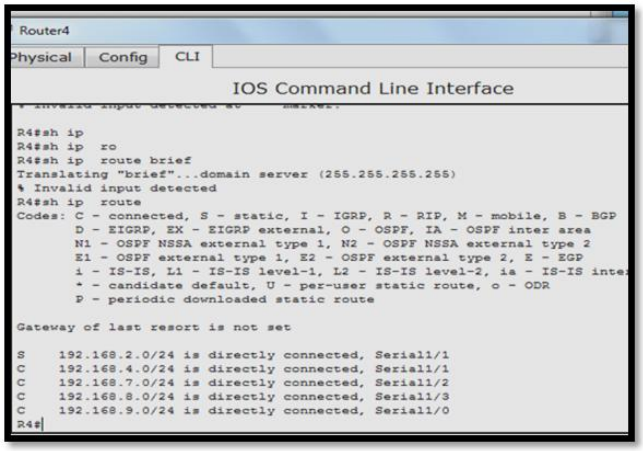

Fig. 6. Routing Table for the node "D".

Fig. 7. Routing Table for the node "D", indicating the failure for the Link Between C and D.

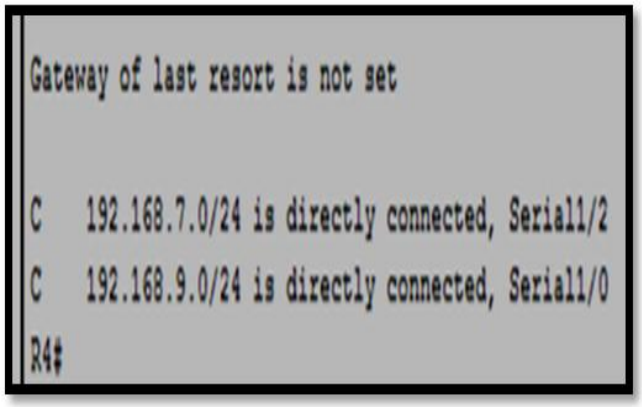

Fig. 8. Routing Table for the node "D", indicating the failure for the Links Between C and D, A and D.

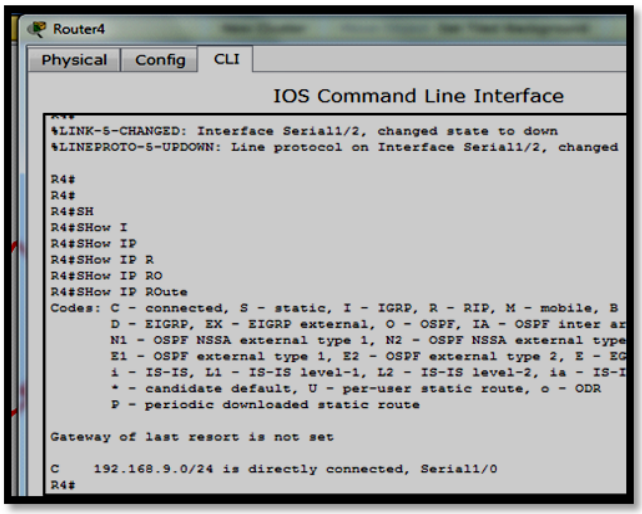

Fig. 9. Routing Table for the node "D", indicating the failure for the Link Between C and D, A and D, and the nodes B and D.

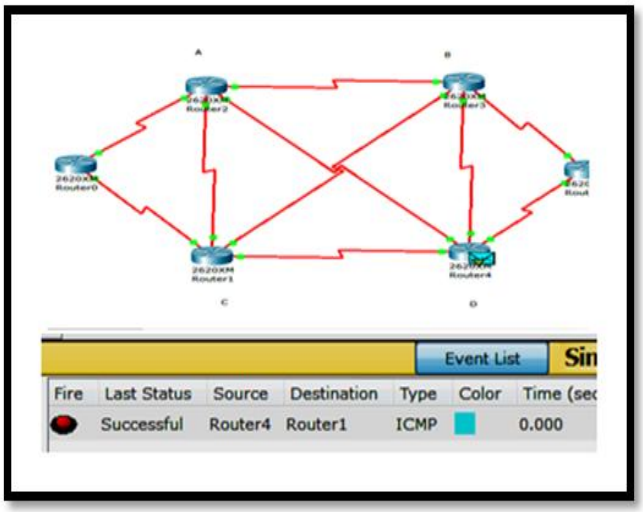

Fig. 10. Successfully sending Message Between D and C.

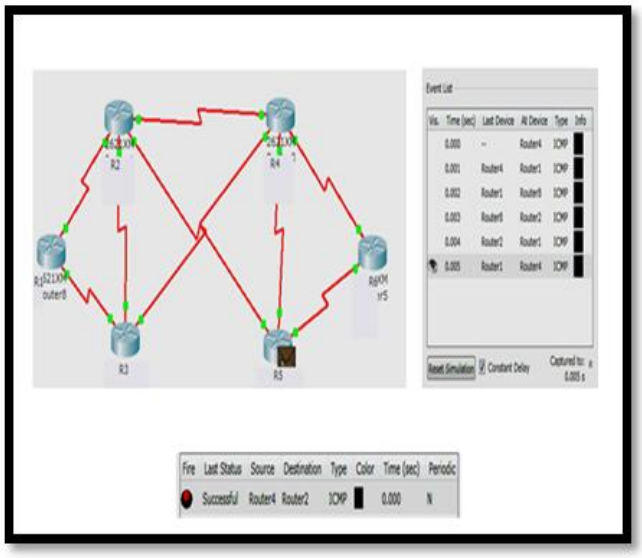

Fig. 11. Successfully sending Message Between D and C, while the Link Between C and D are Down.

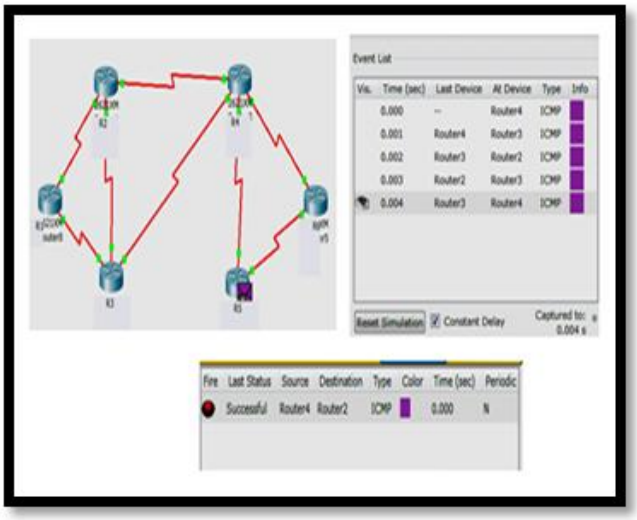

Fig. 12. Successfully sending Message Between D and C, while the Link Between C and D, A and D are Down.

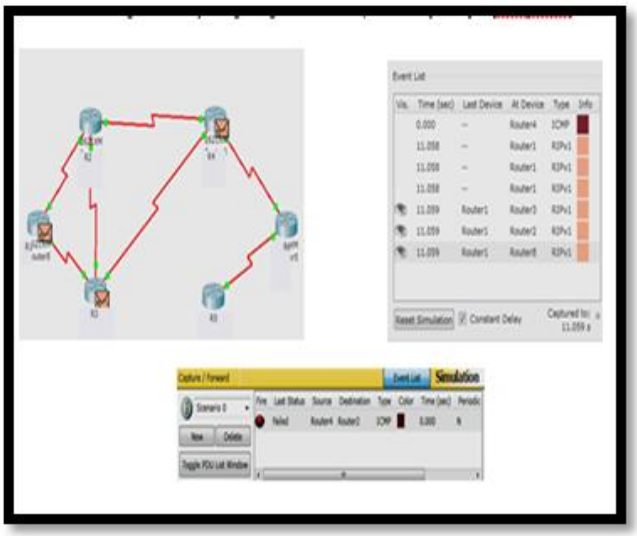

Fig. 13. Failed Sending Message Between D and C, while the LINK Between C and D, A and D and between B and D Are Down.

VIII. RESULTS

The results taken in this paper, shows important issues to be taken in consideration when dealing with intelligent networks, these results could be seen in five main important results, respectively, important of access control list, computer system security, software, applications and the protocol vulnerabilities.

As a result, for Securing intelligent network, which were discussed briefly in section three, it was clear that applying the Access control list for the network is so important, in order to secure both internal and external areas of the network.

Also, the importance of the computer system security, by protecting the data and the information against malicious and unauthorized users by using security concepts as password and applying encryption and authentication algorithms, in order to protect the system any attacker to gain access to the organization data and information, and this was quite clear in section four.

Whereas, the software scenario applied in section five gives an important result, by showing the power of Linux Operating system and its robustness and this was quite similar to the result taken in [12].

Also, the important of choosing the right applications is a relevant task, because many attackers use the vulnerabilities of these applications used by the customers in order to gain access to their systems.

Finally, the protocols and routing vulnerabilities are the main purpose of these results, and it is calculated through Table- I, showing the network connectivity through the implemented second scenario.

Table- I Network Connectivity.

Link Status	Message Delivery Situation
All links are connected	Successfully delivered
Link Between node C and D are down	Successfully delivered
Link Between node C and D, A and D are down	Successfully delivered
LINK Between node C and D, A and D and between B and D are down.	Failure in delivering

IX. DISCUSSION AND CONCLUSION

The Intelligent Network is a computing system that supports Internet service as advanced ability, its vulnerability and security problem should be taken in consideration in order to reduce the security risks and to avoid losing data and services. This paper provides a comprehensive analysis about IN system, by viewing in details, problems such as the network structure, the protocol, the software and the application, where two scenarios implemented, the first shows that the Linux operating system is more secure than windows operating system and this results is quite similar to the results stated in [12], and the second scenario shows the importance of routing and the routing vulnerability, and its results is calculated in Table- I:, this result also is quite similar to the results taken in [6,9,12]. It was clear that the vulnerability analysis results are critical and important to establish more security policy and mechanism, when dealing with IN system.

REFERENCES

1. Olli Martikainen, Juha Lipiäinen and Kim Molin, “Tutorial On Intelligent Networks”, IFIP IN '95 Conference, Copenhagen, Aug. 1995
2. Pooja sharma and Pawan Bhadana, "Advanced Intelligent Network For Wireless Communications" International Journal of Computational Engineering & Management, Vol. 11, January 2011.
3. Xinming Ou and Sudhakar Govindavajhala, " Mulval: A Logic-based Network Security Analyzer", In 14th USENIX Security Symposium, pages 113-128 ,2005.
4. Richard A.Mollin, “The guide to security from ancient to modern time”, Chapman and Hall/CRC; 1st Ed., 2005.
5. Peter Stavroulakis, Mark Stamp, "Handbook of Information and Communication Security", Springer; 1st Ed., 2010.
6. Danfeng Yan, Fangchun Yang, " Vulnerability Analysis of Intelligent Network System", International Conference on Networks Security, 2009.
7. Frédéric Patricelli, James E. Beakley, Angelo Carnevale, Marcello Tarabochia," Disaster Management and Mitigation: the Telecommunications Infrastructure" Jan-2009, Blackwell Publishing Ltd
8. Moore, T. Kosloff, T. Keller, J. Manes, G. Shenoi, S." Signaling system 7 (SS7) network security", Circuits and Systems, MWSCAS-2002. The 2002 45th Midwest Symposium, Aug. 2002.
9. G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi, "Securing SS7 Telecommunications Networks", Proceedings of the 2001 IEEE
10. Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5{6 June 2001.
11. M. P. Clark," Networks and Telecommunications Design and Operation", Second Edition, 1991, 1997 John Wiley & Sons Ltd.

12. Ahmed Refaat Sobhy, Abeer Twakol Khalil, Mohamed M.Elfaham and Atalla Hashad" UAV Cloud Operating System" MATEC Web of Conferences 188, 05011,ICEAF-V 2018.

AUTHOR PROFILE

Ahmed Refaat Ragab is a Doctor Engineer at the Faculty of Information Systems and computer Science, October 6 University. He was graduated from Air Defense College, then he had earned a diploma in computer engineering, from the National telecommunication institute in Egypt with very good grades, and master degree in computer engineering from the college of engineering at the Arab Academy for Science and Technology and Maritime Transport, with EXCELLENT degree and the thesis title was " Secure Routing In UAV". Finally, he obtained the Degree of Doctor of Philosophy in Electrical Engineering, from the faculty of engineering, Benha University, with an excellent degree, and the thesis title was" UAV Cloud Computing System". He works as a lecturer for Communication Network, Electronics, Digital Image Processing and Distributed Systems at the faculty of information systems and computer science, October 6 University, also teaching Cisco courses as an instructor for cisco academy in October 6 university.