Journal of Information Systems and Communication
ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, 2012, pp.- 167-169.
Available online at http://www.bioinfo.in/contents.php?id=45

ANALYSIS OF DICTIONARY ATTACK ON WIRELESS LAN FOR DIFFERENT NODES

VINAY BHATIA[1*], DUSHYANT GUPTA[2] AND SINHA H.P.[3]

[1]Baddi University of Emerging Sciences and Technology/ECE, Solan, India
[2]Electronic Science Department, University College, Kurukshetra University, Kurukshetra, India
[3]M.M.University/ECE, Mullana, India
*Corresponding Author: Email- vinay4research@yahoo.com

Received: January 12, 2012; Accepted: February 15, 2012

Abstract- Wireless LAN deployment has shown an unprecedented growth in recent years. With Wireless LANs users can access mutual information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. WLANs offer various advantages over conventional wired networks, viz., efficiency, service, handiness, and cost. However, vulnerability of WLANs to various attacks discourages the user to use these networks for specific applications. In this paper, we have explored the simulation of a popular WLAN standard, when it is being subjected to the dictionary attack. Here the security protocol has been implemented through Network Simulator-2 (NS-2) Simulation Software and efforts have been made to analyze its impact on the vulnerability to dictionary attack. We have typically implemented WEP and have also studied the effect of this security algorithm on a wireless scenario. The simulation results have been utilized in the development of the analysis of these attacks for different number of nodes.
Keywords- Initialization Vector, TKIP, wireless LAN, wireless security, WEP

Citation: Vinay Bhatia, Dushyant Gupta and Sinha H.P. (2012) Analysis of Dictionary Attack on Wireless LAN for Different Nodes. Journal of Information Systems and Communication, ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, pp.- 167-169.

Introduction

Over the last few decades, wireless networks have been adopted very promptly. Wireless LANs can be found everywhere from offices to homes, from university campuses to cafes and from public buildings to private dwellings. A wireless LAN clubs various network devices to one another without the need of any physical links [1]. "Fig. (**1**)" shows a typical wireless scenario providing wireless networking among different devices henceforth called nodes. However with use of these networks the need of security in these networks is a recent concern. The default protocols currently are being used for the purpose of providing security that suffer from significant flaws, as a result of which, wireless security appears as an oxymoron. Although millions of wireless LANs are in use globally, still it seems counterintuitive that we can deploy and use securely a network with no physical way in barriers. The reason of large deployment of these networks paying no heed to the security issues is due to mobility and freedom they provide. The ubiquity of wireless LANs has lead to a significant amount of research in the field of wireless LANs [2, 3].

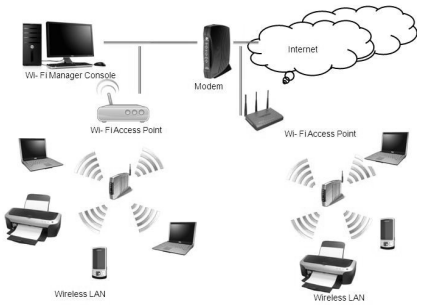

Fig. 1- A Typical Wireless Scenario

To realize a wireless LAN and the advantages it offers over wired counterpart, we must understand potential attacks against it. In this paper we discuss a popular attack against the wireless LAN; the dictionary attack and obtain its effect on a wireless LAN with different number of nodes. Although IEEE organization standard which defines wireless networks communication, has proposed a protocol IEEE 802.11 to offer some wired-like security services,

such as: data privacy, data integrity, and authentication. Unfortunately, this protocol falls short of these objectives, and is vulnerable to many threats which were exploited from time to time [4, 5]. WEP cannot meet the security requirement of WLAN because it suffers from various security flaws. With the fast development of WLAN, the flaws in WEP are exposed gradually which are discussed in the subsequent section.

Security Flaws In Wireless LAN Protocol

In general wireless LAN, users incorporate wired equivalent privacy (WEP) as a security algorithm. The WEP was designed to provide the security equivalent to that of a wired LAN in a wireless LAN. WEP uses RC4 algorithm to safeguard the data transmission against eavesdropping. RC4 is not specific to WEP; it is a random generator and is known as a stream cipher. Although, RC4 falls short of the high standards of security, some systems based on RC4 are secure enough for practical use. In addition CRC-32 is used for integrity check. The wireless LAN standard WEP suffers major security flaws due to improper implementation of the underlying standards [6]. Since its inception various flaws have been reported in WEP by the researchers. The key flaws in this wireless LAN standard are provided subsequently.

RC4 Algorithm

RC4, a stream cipher designed by Ron Rivest in 1987 for RSA Security is a variable key- size stream cipher. This algorithm is based on the use of a random permutation of the key. The algorithm uses eight to sixteen machine operations per output byte.

In this algorithm a variable-length key of 8 to 2048 bits (1 to 256 bytes) is used to initialize a 256-byte state vector S. S[0], S[1],..., S[255] form the elements of the state vector S. At a given time, S contains a permutation of all 8-bit numbers from 0 through 255. For encryption as well as decryption, a byte n is generated from S by selecting one of the 255 entries in a systematic fashion. However RC4 algorithm is used irrelevantly. There is no measure taken to avoid the reuse of key and thus is vulnerable to attacks. Moreover, the RC4 algorithm doesn't have the capability of synchronization. Finally, the mode of key generation is so simple that it is easily exposed to the attack from relative key.

Key Management

The 802.11 standard does not specify how to accomplish distribution of keys. There is no prescription for the generation and renewal of key. In absence of proper key management the keys tend to be long lived and trim down the security.

Initialization Vector Space

The initialization vector space in IEEE 802.11 standard is very small. The initialization vector IV is of 24 bits only. A 24-bit binary string has only 16777216 possible combinations. Due to this small initialization vector IV length the shared key repeats after a comparatively small time interval. Thus there is immense possibility that large numbers of packets are encrypted by the same key. Such packets if captured by an intruder allow him to figure out the secret key and thus the security is compromised.

Inappropriate Integrity Check Algorithm

The IEEE 802.11 employs CRC-32 for providing integrity check. CRC-32 is appropriate checksum for detecting errors, but an awful choice for WEP as it is used for cryptographic hash. Better designed encryption systems such as MD5 or SHA-1 would be better choice.

Dictionary Attack

A Dictionary attack is a password cracking method in which every single word from a word list is tried. A word list consists of large number dictionary words where each word is tried against the password. A simple subclass of dictionary attacks is plaintext attacks [7, 8], where an intruder intercepts a message {M}K encrypted with a weak password K and whose encrypted content M is known (for instance an instruction like hello). The intruder can then try to decrypt this ciphertext with each word in a dictionary one by one, and verify for each guess d whether the value obtained is the known plaintext M, which means with a high probability that d = K. This method also works against a challenge-response scheme where a server sends to a user A a nonce N as a challenge and user A responds with {N}K, where K is its a weak password. In this section we discuss the Dolev-Yao model, Naive Vote Protocol, Offline and Online dictionary attacks.

Dolev-Yao Model

In most approaches concerning automated verification of security protocols, the underlying cryptographic primitives are based on the Dolev-Yao model [9]. In this model, a malicious agent called intruder is assumed to have a complete control over the communication network; he is able to eavesdrop and replay messages, impersonate honest agents, generate nonces. The sequent m means that if the intruder knows the messages in D ⊆ D (F), then he can deduce the message m ∈ D (F). In this model, the intruder can form pairs and cipher texts from known terms, decompose pairs, and decrypt cipher texts only when he can deduce the decryption key. This condition is known as the perfect cryptography assumption.

Naive Vote Protocol

Let us consider the naive vote protocol in which the voter X encrypts a vote V with a public key $^{pub}(K)$ of a vote server S.

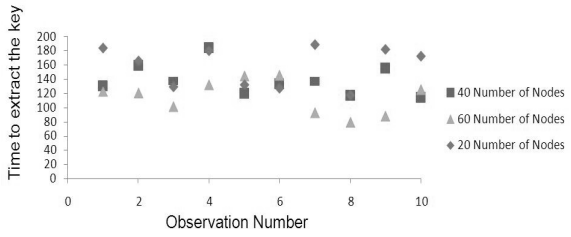

Fig. 2- Total time to extract the key for different number of nodes as a function of observation number

$$X \rightarrow S : \{V\}_{pub(K)} \quad (1)$$

The server S decrypts the message with his private key $^{priv}(K)$ and registers his vote. The protocol is protected as long as only X and S know V. The naive vote protocol is secure in the Dolev-Yao model, because even if the intruder intercepts the message $\{V\}_{pub(K)}$, he is unable to decrypt the message as long as the

private key $_{priv}(K)$ is not known to him. However the situation changes if the intruder knows a finite set D of the values that V can take. Now he can work out V without knowing the private key $_{priv}(K)$ For each value $d \in D$, he encrypts d with public key $_{pub}(K)$ and verifies whether the resultant cipher text $\{d\}_{pub(K)}$ is equal to $\{V\}_{pub(K)}$. Thus he can guess $d = V$.

Offline Dictionary Attack

The challenge-response protocol is vulnerable to a password-guessing attack. In this kind of attack, we assume that an intruder has already built a database of possible passwords, called a dictionary [7]. The intruder eavesdrops on the channel and records the transcript of a successful run of the protocol to learn the random challenge and response. Then the intruder chooses passwords from the dictionary and attempts to produce a response that goes with the recorded one. If there's a match, the intruder has successfully guessed A's password. After each failed matching effort, the intruder picks a different password from the dictionary and replicates the process. This non interactive form of attack is known as the offline dictionary attack.

Online Dictionary Attack

Sometimes an intruder might try diverse user IDs and passwords to log in to a system. For popular Internet services like Yahoo!, the intruder can trivially choose any reasonable user ID due to the large number of registered users [7]. An intruder can also find user IDs within interactive Web communities such as auction sites. If the system rejects the password as being incorrect for that particular user, the intruder picks a different password from the dictionary and repeats the process. This interactive form of attack is called the online dictionary attack

Simulation Parameters and Results

Simulation of a wireless LAN forms an important part of our work. We have typically simulated a wireless LAN of different nodes. The security algorithm used in these LANs is WEP with a total key size of 64. The simulation time used for each simulation is kept constant with a value of 50 seconds. The second phase of simulation is simulation of the most popular attack that is dictionary attack. These simulations are carried out in NS2 simulator. Three wireless LANs are simulated with number of nodes 20, 40 and 60. Each wireless LAN is subjected to dictionary attack for ten times and the total time to extract the secret key is found and the results are plotted in "Fig. (2)".

From the variations obtained in "Fig. (2)" the average time to extract the key per symbol τ_s is found out. In the next step this average time to extract the key per symbol is plotted versus the number of nodes N. These values are plotted in "Fig. (3)". Finally the dependency of average time to extract the key per symbol τ_s on number of nodes or the size of a wireless LAN is found out. Thus the average time to extract the key per symbol is found to be a polynomial function of size of the wireless LAN. Consequently the dependency is given in the following equation.

$$\tau_s = -9\times10^{-5}N^2 - 0.009N + 2.692 \quad (2)$$

As found from equation 2 the average time to extract the key τ_s from a wireless LAN with a default security algorithm implemented using a dictionary attack depends on the size of a wireless LAN and the dependency is found to be a polynomial function.

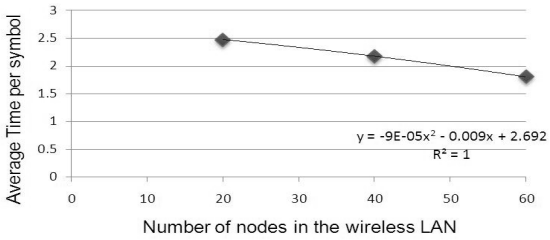

Fig. 3- Average time per symbol to extract a key using dictionary attack as a function of number of nodes in wireless LAN

Conclusion

A wireless network provides number of advantages to the users and a wireless LAN is the most popular form of a wireless network which has widespread deployment. An important parameter of a wireless LAN is its size; whose effect on security is analyzed in this paper. A wireless LAN is susceptible to various attacks due to use of radio frequency waves. The popular attack which exploits the user's tendency to use weak passwords is known as dictionary attack and has been elaborated in this paper. Using the simulation results it may be concluded that the size of a wireless LAN does affect the vulnerability of a wireless LAN. We have found that vulnerability measured in term of average time to extract the key is polynomial function of number of nodes. Finally we conclude that average time to extract a key in a wireless LAN implementing WEP security decreases with an increase in the size of a wireless LAN.

References

[1] Kapp S. (2002) *IEEE J. on Internet Computing*, 6(1), 82-85.
[2] Wool A. (2004) *IEEE Transactions on Wireless Communications*, 3(5), 1459-1462.
[3] Guelzim T. and Obaidat M.S. (2009) *IEEE/ACS International Conference on Computer Systems and Applications*, 251-259.
[4] Arbaugh W.A., Shankar N., Wan Y.C.J. and Kan Zhang (2002) *IEEE Journal on Wireless Communications*, 9(6), 44-51.
[5] Williams J. (2001) *IEEE Journal IT Professional*, 3(6),91-95.
[6] Petroni N.L. and Arbaugh W.A. (2003) *IEEE Journal on Security & Privacy*, 1(1), 28-36.
[7] Delaune S. and Jacquemard F. (2004) *IEEE 17th Computer Security Foundations Conference*, 2-15.
[8] Vykopal J., Plesnik T. and Minarik P. (2009) *IEEE International Conference on Future Networks*, 23-27.
[9] Dolev D. and Yao A. (1983) *IEEE Transactions on Information Theory*, 29(2).