Volume : 2 | Issue : 2 | Feb 2013 • ISSN No 2277 - 8179

Research Paper

Computer Science

KEYWORDS : Password, email, back up, encryption, unlicensed software, awareness of security, wireless network

A study on awareness level of security system in wireless network will influence message communicating inhabitants with special reference to Coimbatore district

S. Lakshmi Priya — Asst. Prof., SIMS & PhD[PT] Research Scholar[CS], Karpagam University.

Dr. R. Lawrance — Director, MCA Department, ANJA College, Sivakasi.

ABSTRACT

Nowadays security plays an imperative responsibility in wireless network since the routing of information is through air. Many encryption methods were developed and are still developing by the research people to shelter their information from intruder. In the army, navy, military, explore etc., fields their information are secured via latest encryption methods implemented through both hardware and software. So it is not an easy job to an intruder to attack secured messages. But in habitual life numerous inhabitants were not having awareness of information security in wireless network even though they are communicating messages (which require secrecy) with many people. In some explore departments itself, they are verdict scores of problems but ahead of discovery to the solution, the same problems were smelled by intruder and they are receiving appraisal even though they are not the novel researchers. This article discuss about the awareness echelon of security in wireless network influences message communicating inhabitants. This process done by assessment amid inhabitants with a mixture of questions which involves network policies, password, email, encryption, unlicensed software etc.., used to quantify the awareness of security in wireless network.

Introduction

We are in the fast moving world and no one likes even less delay "If it is Delay! It is denied! Is the saying in the security services! So mostly we all use the fast communication channel that is nothing a wireless network, but most people do not aware of weakness of security in wireless network. Though people find gate to address and nurture the security ideas to inhabitants to secure their information in insecure wireless network. All the way back attackers getting more ease than the defenders; an attacker is extremely motivated to succeed in his work without concerning any security damage. Most of the successful organization requires alert and defend in all aspects "Known enemies are better than unknown intruders or attackers". Perhaps enemies are known persons then we can easily predict the intention of attacks. Here the unknown represents we do not know who or how or when they will attack with what resources and for what purpose. It is really pathetic! We only know that they are highly motivated to succeed in their attacks on victims while the victims' greatest motivation is to succeed in their own organization objectives. Victims must defend everything of value in fixed, easily knowable locations while attackers only have to attack one thing of value. Motivation is the key to successful attacks and also for good security against such attacks. We must increase the security motivation in our organizations to approach the motivation of our enemies.

I Hate Security

We all hate security because of the inconvenience and the constraints it puts on us in performing our jobs. Remembering and using passwords, limiting information we may use, locking doors and computers, and having to use cryptographic protection are bothersome and detract from our work for which we are compensated. A popular approach to improve our wireless security attitudes and performance is through security awareness programs.

Suitcase the Best Wireless Network Policy

The effective management of information technology resources is remarkably important to the success of the academic, research, patient care and public service missions of the respective organizations. Because of the inherent nature of the wireless communication, wireless networks require increased cooperation and coordination between campus entities to maximize the technology's benefits to the students, faculty, staff of different organizations, to allow connection to wireless networks in different campus buildings, and eventually, to facilitate the ability to roam from building to building without losing network connectivity. Each organization should frame their own wireless network policies and assigns responsibilities for the deployment of wireless services. Policies should be made with out ambiguity and simply in order to understand easily. Polices should focus on the issues that may arise when using wireless communication.

Policies are subject to change as new technologies and processes emerge

Securing Passwords from intruder

- We can protect our passwords from different form of attack other than "asking" and guessing". A hacker won't sit and try for more than 50,000 unique words to hit upon password but he usually use a script or a program to find it.
- The measure of security must then be "**how many password requests can the automated program make - e.g. per second**". The actual number varies, but most web applications would not be capable of handling more than 100 sign-in requests per second.
- Simple passwords can be hacked easily because of its nature of possible character combinations.
- This is of course a highly insecure password, but how much time is enough for a password to be secure?

- A password that can be hacked in **1 minute** is far too risky
- **10 minutes** - still far too risky
- **1 hour** - still not good enough
- **1 day** - now we are getting somewhere. The probability that a person will have a program running just to hack your account for an entire day is very little. Still, it is plausible.
- **1 month** - this is something that only a dedicated attacker would do.
- **1 year** - now we are moving from practical risk to theoretical risk. Expect NASA or CIA persons we do not have that kind of enemies, nor is our company data that interesting.
- **10 years** - Now we are talking purely theoretical.
- **A lifetime: 100 years** - this is really the limit for most people. Who cares about their password being hacked after they have died? Still it is nice to know that we use a password that is "secure for life"

But let's take a full swing at this. Let's look at "100 year - secure for life". It has good ring to it and it makes us feel safe. There is still the chance that the hacker gets lucky. That he accidently finds the right password after only 15 years instead of 100. It happens.

To create a strong password one person can use the following guidelines:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long?
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

The Cease of Email

Communication is an essential part in every business environ-

Volume : 2 | Issue : 2 | Feb 2013 • ISSN No 2277 - 8179

ment whether it is a small company or a huge enterprise. Aside from meetings, conferences and brainstorming, written communication is very important in all aspects. It is the most efficient way to communicate and send business updates to other employees, superiors, clients, suppliers and important contacts. Sending emails has become one of the most used functions of the internet and in more ways than one, the most helpful as well. Exchanging messages is faster and significantly less expensive. Without the internet, the fastest way to do business and send an important message are via overseas calls, telegram messaging, mailing services or travelling directly to the place or country. Imagine the amount of money and time a businessman has to invest just to communicate with a client or partner and make business possible. With the presence of the internet and email service, sending and receiving messages can be done fast and efficiently without having to spend a lot of money and wasting a second. Productivity and profitability can be increased with faster communication.

Improper Email Habits

While email has enabled companies to market their businesses to a large audience, they should avoid spamming potential clients with endless messages. Instead, emails should be tailored to suit the interests of the potential client. The sender should avoid ccing more people than is truly necessary. There is little that is more frustrating than being copied in an email when the content is irrelevant. Email should never be used to send personal or confidential information—once an email is sent, it can easily be forwarded on to anyone, and could fall into the wrong hands. Email can be a very effective and strong tool if used correctly. Knowing what to avoid is crucial to maintaining professionalism at all times.

Backup Data from workstation

In any organization it is essential to save their unique data. This can be done be regular back up. To back up Information efficiently the organization can follow a schedule method. A good plan is to schedule the same time each week or month to back up data, run a full scan and repair of files followed by a full de fragmentation of the hard drives. Once data has been backed up, remember to apply the same security precautions to the back up (physical security, encryption as needed- if so back up encryption key, etc.) similar to any other type of data. The person who is taking back up can use various devices. He should have awareness of those devices like how to handle, how to protect, where to keep etc...

Securing Information through Encryption

There are various encryption methods are available to secure the messages. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the cipher text, is then transmitted, often by messenger or radio. We assume that the enemy, or intruder, hears and accurately copies down the complete cipher text. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the cipher text easily. Sometime the intruder can not only listen to the communication channel(passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver(active intruder). The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology.

It will often be useful to have a notation for relating plaintext, cipher text, and keys. We will use C = EK(P) to mean that the encryption of the plaintext P using key K gives the cipher text C. Similarly, P=DK(C) represents the decryption of C to get the plain text again. It then follows that DK(EK(P))=P. This notation suggests that E and D are just mathematical functions, K is key. The only tricky part is that both are functions of two parameters, and we have written one of the parameters (the key) as a subscript, rather than as an argument, to distinguish it from the message.

Encryption methods have divided into two categories: substitution ciphers and transposition ciphers. Depends on the requirement any one of the encryption methods can be selected to secure the message from the unknown attacker.

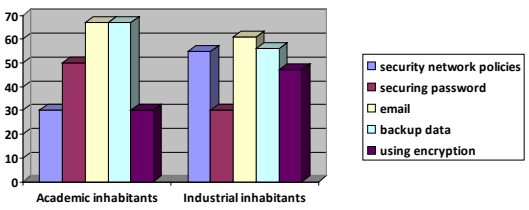
Hypothesis Calculation

Ho- Null hypothesis there is a no need to give awareness program on wireless network security for the message communicating inhabitants.

Ha- Alternate hypothesis there is a need to give awareness program on wireless network security for the message communicating inhabitants.

Here fo denotes the frequency of the observed data and fe is the frequency of the expected values. The general table and its corresponding chart would look likes below:

Type of Inhabitants / Awareness categories	Message communicating Inhabitants- Academic (fo)	Message Communicating Inhabitants - Industrial(fo)	Row total
Security Network policies	30	55	85
Securing password	50	30	80
Email	67	61	128
Backup data	67	56	123
Securing using encryption	30	47	77
Column total	244	249	N=493



Now we need to calculate the expected values for each cell in the table and we can do that using the row total times the column total divided by the grand total (N).

Observed	Expected(fe)	|O -E|	(O — E)^2	(O — E)^2/ E
30	42.07	12.07	145.66	3.46
50	39.60	10.40	108.28	2.73
67	63.35	03.65	13.32	0.21
67	60.88	06.12	37.50	0.62
30	38.12	08.12	65.76	1.73
55	42.93	12.07	145.66	3.39
30	40.41	10.41	108.28	2.68
61	64.65	03.65	13.32	0.21
56	62.13	06.13	37.50	0.60
47	38.89	08.11	65.76	1.69

Chi Square = 17.32

Degrees of Freedom = (c - 1)(r - 1) = 1(4) = 4

Chi Square distribution table Probability level (alpha)

Df	0.5	0.10	0.05	0.02	0.01	0.001
1	0.455	2.706	3.841	5.412	6.635	10.827
2	1.386	4.605	5.991	7.824	9.210	13.815
3	2.366	6.251	7.815	9.837	11.345	16.268
4	3.357	7.779	9.488	11.668	13.277	18.465
5	4.351	9.236	11.070	13.388i	15.086	20.517

Reject Ho because 17.32 is greater than 9.488 (for alpha = 0.05)

Thus, the result says that reject the null hypothesis that is there is a need to give awareness program on wireless network security for the message communicating inhabitants.

Conclusion

Securing password is such a challenging task to protect the confidentiality in any electronic related factor to save the sources and mainly from the intruder has to concentrate on the individual and the software maintainer to meet their expectation. As a concluding example, take a look on the giant machine Google; it always monitors the performance of users in terms of length and duration of the password automatically and periodically respectively. Similarly habitats of email and maintenance are taking care of both individual and software maintainer. Any organization should frame and narrate the security policies to the employees and also to be trained to protect the same. Perhaps any change happen in the company policy will not violate the security system. The information system will be varying organization to organization to maintain the business information. This should be handled by the expert and honest trainer on requirement; an organization can follow liberal encryption methods. At least, this technique should be reached to the organizations which are highly required information security on wireless network. In order to create awareness about these five categories there is a need of awareness program from the expert of respective categories in and around Coimbatore District. In future categories can be increased like licensed software, protect hacking of information etc.., and survey could be conducted in state level to strengthen the security level of wireless network.

REFERENCE

1. "Fighting Computer Crime, A New Framework for Protecting Information," By Donn Parker and published by John Wiley & Sons, | 2. Information security awareness in UAE: A survey paper | 3. http://mathforum.org/library/drmath/view/52756.html | 4. http://email.about.com/od/freeemailreviews/tp/free_email.htm | 5. Doe, Jane. "How to Cite Information from an E-mail." E-mail to Joe Schmo. | Nov. 2003. | 6. Cryptography: A New Dimension in Computer Data Security--A Guide for the Design and Implementation of Secure Systems |