WIRELESS SECURITY MEASUREMENT USING DATA VALUE INDEX

Reza Amirpoor [1] and Ajay Kumar [2] and Satish R. Deavne [3]

[1]Research Student, IMED, Department of Computer Management, Bharati Vidyapeeth University, Pune, INDIA, 411008, Tel No. : +91 9890307927
reza_amirpoor@yahoo.com
[2]Director, JSPM's JAYAWANT Institute of Computer Applications, Tathawade, Pune, INDIA, 411033
ajay19_61@rediffmail.com
[3]Principal, Dr. D. Y. Patil Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, INDIA
satish@rait.ac.in

ABSTRACT

Nowadays, use of wireless technology in organizations is a regular act, and we can see this technology erupted in all possible different areas. Related to employing wireless technology those organizations need to apply properly security level, depend on security policy which already defined. If security system applied but not required, or security system required but not provided, leads to improper security system. In this paper we have shown the way to evaluate the data significant and their appropriate security level. Here a model to evaluate the cost of data on security point of view by consideration of some parameters like sensitivity, volume, life, frequency, etc…, this research makes organizations to predict and implement or understand the cost involved for security of their data by measuring the data value. We used questionnaire and survey methodologies to collect the data; and then used SPSS and SAS program to calculate and design a model. In this way regression and BOOTSTARP help us to find accurate result. .

KEYWORDS

Data Value, Security Policy, Wireless

1. INTRODUCTION

Wireless technologies are increasingly popular around the world, many organizations applied to wireless networks at part of own networks, in recent years, , price of wireless production has been reduced and we can prepare device of wireless network cheaper than wire device.. With respect of this cost and easily to install and also user friendly, organizations looking for wireless networks.

Despite we will take reap of benefits in this way, but security is becoming main challenge. Wireless heritance is more vulnerable than wire technology. With this security concern, we implement security policy related to our organization to cover all angle of breach architecture, and answer to all questions which will come later about security.

The goal of this paper is to make the reader aware of the weakness in current wireless security models and to lay a framework for a reliable wireless security policy for all organizations by any value of the data on security view. To that end, this paper will examine the data and identify the effective wireless security policies. As the number of employees, applications and systems increases, the management of the organization's information becomes much more

difficult and consequently vulnerabilities potentially increase. To determine secure use of hardware and software, as well as, facilitating and encouraging secure employee behaviour, organizations make use of information security policies. An information security policy is a combination of principles, regulations, methodologies, techniques and tools [1] established to protect the organization from threats. These policies also help organizations to identify its information assets and define the corporate attitude to these information assets [2].

2. LITERATURE SURVEY

The security of business transactions and personal data is not simply dependent upon the security of the network. From a survey of small-medium enterprises in Hong Kong,

Chung and Tang (1999) [3], conclude security management is an important success factor for the adoption of information systems in small-medium enterprises. So as new customer-based information systems are designed, developed, procured and deployed the privacy related security issues of the information system needs careful consideration.

With the increasing use of the Internet and mobile technologies by smaller organizations, enabling them to be more flexible and diverse in their operations, the threats are broadening. Effective security management is therefore, essential for all organizations in this increasingly interoperable world in order to ensure that the information remains confidential, available and retains integrity.

Table 1 summarizes level of adoption of security management policies by small businesses. The levels of planning and policy definition are low in comparison to larger organizations. Only 41 per cent of small businesses have written a security policy that will protect customer privacy [4] in comparison to 76 per cent of large organizations [5]. The reasons for this difference relates to expertise, resources, and an understanding of the risk.[6]

Our policy throughout was to ensure privacy of data by ensuring the system and organizations were secure from accidental, deliberate and opportunistic attack. The security policy was based on the international information security standard for best practice (ISO17799).

Table 1 Policies and Procedures Currently in Place [3]

Document	**% of respondents**
Data recovery procedures	47
Computer use and misuse policy	43
Information security policy	41
Information security procedures	33
Business continuity plan	24
Data destruction procedures	21

Organizations need to understand the real risks and build security management policies on them; evaluate technological solutions and external hosting decisions on the total cost of ownership; build systems with defence in depth, where the first line of defence is users who are aware of the issues; and to minimize the chance of unauthorized access by defaulting to a policy of least privilege access and monitoring the network to maintain confidence to ensure the security policy working.

3. SECURITY POLICY

Protection of assets is critical part of each organization. Wireless vulnerable can give anxious to organization about the data. Despite benefit of wireless is always an enthusiasm to remain in organizations.

Changes in technological solutions should be based upon a security policy. Without a policy, security practices will be undertaken without any clear strategy, purpose or common understanding. So important is this area of management that there is now an international standard (IS0 17799) that states the principal tenants of information security management policies, such as ensuring that the policy is aligned to business objectives.

A. Why Policy?

Security policies help organizations to define important assets and specify the appropriate steps to be taken to safeguard those assets. Organizations can benefit from the conveniences of wireless but it's risky from a security standpoint not to have a policy in place to help, to guide the users in the appropriate implementation and use of the technology [7].

A well-written wireless security policy will provide a reference document that will answer users' questions about wireless security and is a document that can be referenced if conflicts arise during the implementation or daily use of the technology. It will provide a centralized location for security guidance and allows for centralized updates as the technology and risks associated with its use evolve. Additionally, the policy should standardize the security practices of the user base. For example, the policy may state that no wireless devices may be taken into areas designated for classified information. This will make it easier for the security department to advertise this rule to users by referencing its inclusion in the policy document, which all users are required to read [8].

In any case, poor security architecture can create conflicts and tensions by unnaturally restricting the user's options. Inferior security components can hinder application growth, and applications might be forced into choosing between business feature support and security. Well-designed applications can catch and address many of these issues successfully at the architecture review.

The major purpose of the security policy is to select the appropriate security solutions to face those threat events while ensuring that the cost of protecting the infrastructure does not exceed the benefit it provides. In business jargon, the rules of the security policy should guarantee a return on investment

4. ADJUST SECURITY POLICY IN ORGANIZATION BY THE DATA VALUE

One expert commented on the budget "One day my boss asked me 'are we protected?', I told him if you have a house and you want to protect it you will need money to do so…

So the level of security or the protection you will get depends on how much money you will spend. According to the budget, we plan for information security". The budget needs to be adequate: "Without enough money, we can't have security in the organization; money will bring software, hardware, and consultants". Without a proper budget, organizations won't be equipped with sufficient resources to ensure information security.

If security system applied but not required, or security system required but not provided, leads to improper security system. In first case we wasted our resource and it make trouble in opposed goal in system architecture. The goals of performance and portability are in conflict with security architecture goal. We will lose that goal by increasing and adding more security system in our organization, and this is force and pressure in total system architecture. In Second case, if we denied implementing properly security system in organization, it means we push our assets to vulnerable field. So we can't protect the data from malicious attack. Table 2 shows the relation between appropriate security level and data value.

First column is security policy levels, start from minimum security to maximum security, in second column we use a model to find the data value which start from minimum value to maximum value. Any level of data value model can compare to same level of security level or one level up, it means any organization can calculate of own the data value and then can find security policy level of those data. Security policy model can use from ITSEC or other standards, but we recommend to use of ITSEC standard. The ITSEC addressed an expanded view of confidentiality, integrity and availability with the aim of more explicitly addressing both military and commercial requirements [9]. Table 2 also can help to prediction of security level need for the organization. By calculating the value cost of data for next few years and you can take security level for those years.

The data value is derived from our model are calculated by a questionnaire, which collected from network administrator of organizations. This questionnaire is useful to put in our model to find data value of security view of the organization's data. In fact data value model is observation of network administrator on the organization's data. Through this observation we can find data value.

Table 2 Relation between Security Levels and Data Value Model

Security policy levels	Data value Model
S1	D1
S2	D2
…	…
Sm	Dn

By finding the relation between data value and security policy, our goal be accessible to define the best security policy level for our organization.

5. MODEL OF DATA VALUE POINT OF SECURITY VIEW

Implementation of security architecture in system should be balanced by the data value of that organization. Before applying security in system, one must know about the data value in system.

The data in any organization have cost and value. Some data is less value and some of them can't take value or price. Some data are looked by hackers and malicious people, to access by different mention. The data is affected by some parameters; we can show this by formula:

- DATA value from security point of view = F(X,Y...) (1)

Which F() is a function included some parameters; these parameters has been effected on the data value; and caused to change value and price of the data. The value of data can calculated by linear function, however, this function (1) should cover whole area atmosphere on data value. These parameters are shown as below (2):

- Sensitivity of data
- Volume of data
- Life of data
- Multiple places of users
- Frequency of use
- Update frequency of data
- Wireless data

All of the seven parameters are affecting on data to get value, but by different coefficient; The data can weight by these parameters, definitely may be more parameter can find and added to this collection, here we have considered only seven parameters to describe the model; these parameters are varying from organization to organization and system to system; it can be high, it can be low or in middle range accordingly we have to apply the security level for cost effectiveness and proper security implementation.
The final model (3) can calculate data value for Table 3 , minimum be 0 and maximum be 8400, which 0 is equal to D level of security level policy (minimum security required) and 8400 is equal to A level of security policy (maximum security required) for the organization.

We should divide and category range of (0 … 8400) to all security level policy, to draw properly relate between data value and security policy.

This model given by:

- DATA value from security point of view = $\alpha + \beta_1 S + \beta_2 V + \beta_3 L + \beta_4 M + \beta_5 U + \beta_6 F + \beta_7 W + \varepsilon$ (3)

    - α = Intercept cost of Data
    - S = Sensitivity of Data
    - V = Volume of Data
    - L = Life time of Data
    - M = Multiple places users
    - U = Updated Frequency of Data
    - F = Frequency of Data used
    - W = Wireless Data
    - ε = Hidden parameter cost

Which $\beta 1 ... \beta 7$ are coefficients on parameters. By regression calculation and SPSS software, we have derived those coefficients.

A. Methodology and Empirical Evidence

Our research is aimed at all companies, which used wireless technology for communication; the interview was arranged and conducted with all of the participants at the convenience of the interviewee and took place in the interviewees' offices. Confidentiality of the data was guaranteed. All participants requested that anonymity also be guaranteed.

Thirty six organizations selected in six different areas to collect the data; these six areas cover all variation of organizations which have data by different value. These are as below:

- Educations
- Research places
- Business
- Medical
- Industry
- Citizen Service

All of them used wireless technology as basic part of own networks. We collected the data value of 36 organizations through questionnaire and survey; network administrator in all organizations responsible for those questions, through these questionnaire we tried to collect effective of parameters on value of data on security view by administrators of organizations, and take their observation on the data value.
Table 3 shows the variation of data value collected by questionnaires on different area which already defined. Depend on inherently of area these data value should be changed. Despite security level required also is changed. In Table 3, we can see maximum security level required is on the business row and also in education level. In these two categories we should apply maximum security policy level.

Maximum data value which we collected is 6400 in bank category, and minimum value is 790 in industry category.

Table 3 Tabulation of Data Value Range in Different Area of Wireless Users

Range of value	Min. Value	Max. Value
Education	1530	4960
Research	3075	3720
Medical	2460	2720
Citizen Service	1080	2910
Industry	790	2720
Business	6240	6400

Each parameter through questionnaire designed 1200 score and maximum value on each organization is 8400 (7 * 1200).

B. Analyze of Data

Figure 1 shows the variation of value of different parameters on the data value, each parameter has specific effect on the data value. Sensitivity and life of data on organizations are important parameter which can increase the value of data on security view. Update frequency of data is less effect on the data value from security point of view. In some area as citizen service don't need more security level, because no one of the specifics is high and average of all seven parameter (2) is in half down of Table 2. In this case, we can apply minimum or like this to security organization. Business area included bank is in high level of security, and consequently must apply maximum security level on this organization.

Figure 2 shows the three parameter cover 45 per cent of total value of data. These parameters are wireless data, sensitivity of data and multi places of data.

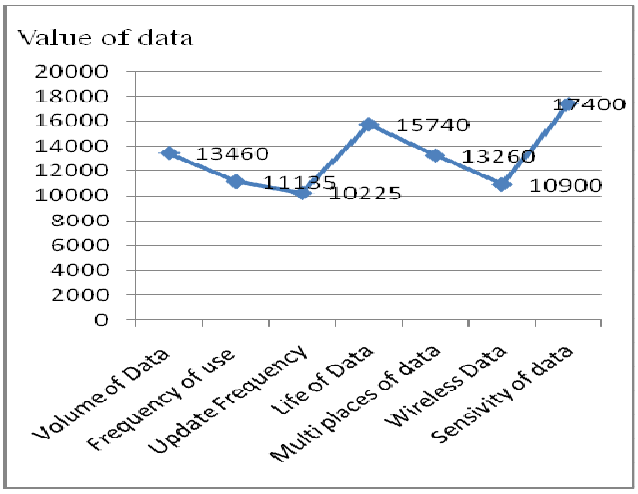

Figure 1 Different parameter by different coefficient on total data value

A common specific on these three is all of them use various users, and consider by hackers.

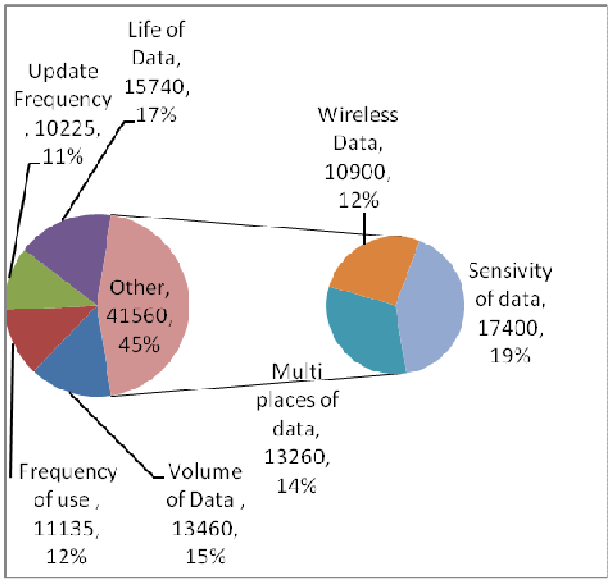

Figure 2 Percentage of different parameter

In questionnaire designed different way and different question to take value of each parameter; our mentioned is to define common coefficient for each parameter for only one formula, and finally we can apply this formula to every organization.

We used SPSS and SAS to find coefficient, SPSS used to make components of our parameters, result be as below:

Component 1= (freq *.852) + (update-freq *.886) + (life* .604). (4)
Component 2= (volume * .858) + (multi-places * .750).
Component 3= (wireless * .920) + (sensitivity * .716).

Three parameters of them (frequency of use, update frequency of data and life of data) make a component and volume of data and multi places of users are another component and the last wireless data and sensitivity of data are a component. Each component is elaborate included parameters in the same level, and they can be in same range of effectiveness.

We have written a program for SAS application to use a bootstrap methodology for help us in this way, bootstrap used 100 000 resample of this 36 observation. Bootstrap helps us to find accurate result. By this methodology we have got the coefficients of all parameters.

A program for SAS to compute a coefficients and variants through BOOTSTRAP methodology is written; and apply to inference coefficient of our components. By 100 000 resampling model and 36 observation finally we got result of our model. This model given by:

Formula (3) will be completed by: -3334 + F (I, S, V, L, M, U, F, W);

And final model be:

$$= -3334 + 8.29\,F + 8.62\,U + 5.88\,L + 20.97\,V + 18.33\,M + 11.71\,W + 9.11\,S; \qquad (5)$$

Formula (5) is a common formula to take value of data on security view on every organization, and through this result and use Table 2, we can adjust our security policy on organizations.

Now we can use this model to find accurate data value of security point on our observations; the result shown in Table 4. Maximum score is for business group and minimum came in industry and citizen service groups.

Table 4 Tabulation of Data Value Range in Different Area of Wireless Users Used Formula (5)

Range of value	Min. Value	Max. Value
Education	2538	3971
Research	2516	3586
Medical	1168	2759
Citizen Service	728	4070
Industry	106	4021
Business	4606	4958

But as in above table we can see in some industry area also have high data value; and depend on organization and data value we can apply for security level, and through Table 2 and adjust between security levels and data value we can find level of security in our organization and we can apply or modify on that level.

6. CONCLUSION AND FUTURE AREAS OF RESEARCH

With the myriad of security issues facing wireless technology there is a need for strong and effective wireless security policies. Fortunately, while there are many wireless security policy templates available, this paper has shown how to select the best security policy for own organization, and discussed the weakness and strong in select properly security policy and proposed a framework for a reliable wireless security policy for all organizations by any level of data value. Near 45 per cent of data value from security point of view is included of Wireless, Multi places users and Sensitivity of organization's data. Any organizations use out of these three specific of data should use top half of security level model for own organization.

In this paper, we have developed a model to estimate a data value point of security view on organization. This model allow the systems to find the best security model for own organizations. Applying this model to system security design will improve system security performance and decrease the overheads in nearly every security related area. This model to evaluate the cost of data on security point of view by consideration of some parameters like sensitivity, volume, life, frequency, etc…, this research makes organizations to predict and implement or understand the cost involved for security of their data by measuring the data value.

Because this is the first time we try to model the data value, there are some important works that we can calculate the data value for different area by different security policy in the future. It helps to define and implement appropriate security policy for all organizations. Also we can suggest new parameter which can be effect on the data value on security view, and redesign our model.

REFERENCES

[1]. Tryfonas, T., Kiountouzis, E. and Poulymenakou A, Embedding Security Practices in Contemporary Information Systems Development Approaches. *Information Management & Computer Security*, Vol. 9, No. 4, (2001) 183-197.

[2]. Canavan, S., An Information Security Policy Development Guide for Large Companies. *SANS Institute,* 2003.

[3]. Chung, C-W and Tang, Computer Based Information Systems (CBIS) adoption in small businesses: Hong Kong experience and success factors, *Journal of Global Information Technology Management*, M-ML (1999), *2*(2) 5-22.

[4]. Gupta, A. and Hammond, Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination ,*Information Management &Computer Security*, R. (2005), *13*(4) 297-310.

[5]. Fulford, H. and Doherty, The Application of Information Security Policies in Large UK-based Organizations: An Exploratory Investigation, *Information Management & Computer Security, N. F. (*2003) , *11*(3) 106-114.

[6]. Ian Allison, Privacy through Security: Policy and Practice in a Small-Medium Enterprise, The Robert Gordon University, UK.

[7]. MICHAEL MANLEY, CHERI MCENTEE, ANTHONY MOLET, AND JOON S. PARK. A FRAMEWORK OF AN EFFECTIVE WIRELESS SECURITY POLICY FOR SENSITIVE ORGANIZATIONS. IN *PROCEEDINGS OF THE 6TH IEEE INFORMATION ASSURANCE WORKSHOP (IAW)*, IEEE COMPUTER SOCIETY WEST POINT, NEW YORK, JUNE 15-17, (2005)150–157.

[8]. Jay Ramachandran, Designing Security Architecture Solutions, WILE, 2006.

[9]. An Oracle White Paper, Computer Security Criteria: Security Evaluations and Assessment, July 2001.

Authors

Reza Amirpoor received the B.E. degree from Sharif University of Technology in 1996 and MBA (IT) degrees, from Symbiosis International Univ. in 2006. He is Ph.D. student in Bharati vidyapeeth Univ. in PUNE since 2007. His research interest includes Computer Networks, wireless systems and security systems.

Dr. Ajay Kumar has completed M.Sc. Engg. in Computer Science and Ph.D. He is having 21 years of teaching and research experience. Presently he is working as Director, JSPM's JAYAWANT Institute of Computer Applications, Pune-India, He has published four books in Information Technology. He has also published more than 35 papers in National / International Conferences and Journals. His area of research is Computer Networks, mobile computing, wireless systems, security systems and Software engineering.

Dr. SATISH R. DEVANE has completed M.E. Electronics, from Dr. B.A. M University, Aurangabad and Ph.D. in Information Technology from IIT Bombay 2006. Presently he is working as Principal, Dr. D. Y. Patil Ramrao Adik Institute of Technology, Nerul, Navi Mumbai -India, He has published one book in Computer programming. He has also published more than 20 papers in National / International Conferences and Journals. He has Life Membership in IEEE, ISTE, CSI, IETE, ISACA, Security Technology Forum of CSI. His area of research is E-Commerce, Computer Organization, Network Communication, Web Technology, Smartcard, System Analysis and Design, Operating System, Network Security, Software Engineering.