roar @UEL
research open access repository

University of East London Institutional Repository: http://roar.uel.ac.uk

This paper is made available online in accordance with publisher policies. Please scroll down to view the document itself. Please refer to the repository record for this item and our policy information available from the repository home page for further information.

Author(s): Ijeh, Anthony C.; Preston, David S.; Imafidon, Chris; Williams, Godfried
Title: Security strategy models (SSM)
Year of publication: 2009
Citation: Ijeh, A.C. et al (2009) 'Security strategy models (SSM).' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 4th Annual Conference, University of East London, pp.126-131
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/FinalProceedings.pdf

SECURITY STRATEGY MODELS (SSM)

Anthony C. Ijeh, David S. Preston, Chris Imafidon, Godfried Williams
School of Computing, Informarion Technology & Engineering, University of East London
a.ijeh@uel.ac.uk, d.preston@uel.ac.uk, c.o.imafidon@uel.ac.uk, g.wiliams@uel.ac.uk

Abstract: The aim of this research paper is to analyse the individual and collective information security risks which could arise from using a security strategy model (SSM); the objective of creating the SSM was so as to protect a wireless local area network (WLAN). As such the focus of this paper shall be on the individual operational components used to create the SSM and the information security risks which stem from their being part of the SSM. In order to review the components of the SSM the paper shall use the BS ISO/IEC 17799:2005 which is the British Standard, International Standard and also the European Standard for using Information Communication Technology (ICT) correctly in order to effectively mitigate against the exposure of an organizations data to unauthorized access. The general idea of using the BS ISO/IEC 17799:2005 is so that the SSM is created based on best practice within the ICT industry of protecting confidential data or at least that the possible risks that stem from using the SSM are mitigated against; this is also known as risk based auditing. Against this backdrop the paper shall review each component of the SSM and use the risks to create a 'Threat' model which would then be used to create a 'Trust model in order to strengthen the confidentiality of any data that passes through the SSM.

1. Introduction:

Most issues arising in creating security strategy models (SSM) have been linked to the physical security of systems, protocols and policies according to recent research. However in contrast to this it has been suggested that the non inclusion of human behaviour as components in these SSM's has been the cause of key risk issues (Ustan, Yilmaz et al. 2006). This is because as the paper suggests without the inclusion of a component that caters for the behavior of human beings in modeling the security of systems, then it is not possible to effectively apply the process agents that are used in developing an effective security strategy model. In addition to this other research has suggested that one such area of the need to consider human behaviour when creating security strategy models is in wireless communications. This is due to data from wireless networks being transmitted between devices through the air via radio waves, which are susceptible to interception from unauthorised persons. Solutions are consistently been sought for these problems with the emergence of IT Governance (ITG) and Wi-Fi Protected Access Protocols (WPA2). In order to deal with these deficiencies researchers have suggested that more consideration is given to the basic concepts of security modeling experimental design, as the types of goals to be addressed are so important and useful to the objectives of the security modeling simulation. The researchers argue that the justification for this approach is because security models are developed through this research approach (experimental design) and that a well designed experiment allows the analyst or researcher to examine many more factors than would otherwise be impossible (Sanchez 2007). In comparison to this other academia have suggested the use of risk based security values when designing security model prototypes (Pedegraft,

Rounds et al. 2005); their research suggests that due to the changes that occur over time in the use of Information Technology (IT) and systems which can be positive or negative changes; that security values e.g. IT security policies should not be used in isolation but based on the activity of the IT systems being used. In order to develop an efficient security strategy model (SSM) the above literature suggests that there is a need to understand both human and non human factors that stem from the usage of the system to which it is being designed to protect. The aim of this paper is to use the components of an already designed SSM and use the risks which could stem from its usage to create a 'Threat' SSM model which would then be used to create a 'Trust SSM model in order to strengthen the confidentiality of any data that passes through the SSM. In order to justify and test the SSM pre and post its implementation a known problem will be used to develop it and then IT Audit standards (BS ISO/IEC 17799:2005) will be used to test if it meets industries best practice.

2. Wireless technologies:

In order to understand the usefulness of SSM's it is helpful to identify an already existing problem that they can be used to solve. Wireless technologies have undoubtedly brought about an increase in the ability and convenience of using mobile technologies to process data. However, processing data that is not physically controllable has privacy risks. To date, wireless technologies have not been able to restrict the radio waves that are used to transmit data from one access point to another from leaking through the windows and doors of an organisations building. A research paper by (Stubblefield, A. et al. 2004) details findings on how a practical key recovery attack on Wired Equivalent Protocol (WEP), based on partial key exposure vulnerability in the encryption being used (RC4 stream cipher) can be used as a flaw in breaking WEP. The paper describes how to apply the flaw in breaking WEP and concludes that the protocol also referred to as 802.11b WEP standard by the Institute of Electrical and Electronic Engineers Inc, is not secure. Information from this paper suggests that current WEP problems which are still being experienced as WEP is still widely being applied by organisations and home users make the use of WEP a threat to the integrity of confidential data held on any network using it as their protocol. Another research paper by (Hori, Y. and Sakurai, K. 2006) specializing in the WPA and WPA2 Protocol, details findings on why the WPA protocol was developed and what vulnerabilities it was created for. The paper further describes that the WPA adopted the key management system or Temporary Key Integrity Protocol (TKIP). The paper however suggests that the protocol uses keys generated by the server, which even though dynamically created still leave room for the keys to be hacked into. This study acknowledges the use of Message Integrity Checks (MIC) in order to mitigate against the keys being cracked. However, there is still room for unauthorised persons to break into the network via these distributed keys. Information from this article will help us support our research proposal that suggests that the current protocols whilst bring a management framework by which the wireless technologies can be governed cannot provide the required security as there is still signal leakage which allows unauthorised persons to access the organisations network and view confidential data. The next step is to collect the data from the wireless technologies in the proposed

Security risks to wireless technologies: Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or "layer" of the network.			
Dependent Variables	**Data Measure of Dependent Variable**	**Independent Variables**	**Data Measure of Independent Variable**
Threat Model		War driving, walking, spying and flying	

Table 1: Wireless Technologies 'Threat Model'

experiment. Data analysis in experimental research comes down to calculating "correlations" between variables, specifically, those manipulated (Independent) and those affected by the manipulation (dependent). Only experimental data can conclusively demonstrate causal relations between variables. Table 1 identifies the dependent and independent variables for risks to data transmitted by wireless technologies

3. Security Strategy Model (SSM):

So far in this paper, researchers have acknowledged that privacy is critical to the security of data transmitted by wireless technology. However there has been no technology to date that has been able to prevent the radio waves from transmitting data out of an organisations building. This section aims to propose a security strategy model as a solution to the areas that threaten wireless data security as shown in Table 1; that affects the ability of Wi-Fi technology to secure the data transmitted over wireless communications. This papers proposed security strategy model is already in use in most hospitals in the United Kingdom (UK) and is based on location based services (LBS). Recent research (Chen, Y. and Chan, Y. et al. 2005) suggests that the LBS technology can be developed in a way that is of value to this paper, and that is that they can be used to monitor wireless test beds. In addition to this researchers have used data models to accommodate spatial values that exhibit partial containment relationships instead of total containment relationships (Jensen, Kigys et al. 2002). This finding is important to this authors study as he intends to use relationships of the variables from his results to show causal relationships between the data. Table 2 identifies the dependent and independent variables for risks to the components of the security strategy model (SSM)

4. IT Governance (ITG) Standards for SSM:

In order to review the components of the SSM the paper shall use the BS ISO/IEC 17799:2005 which is the British Standard, International Standard and also the European Standard for using Information Communication Technology (ICT) correctly in order to effectively mitigate against the exposure of an organizations data to unauthorized access.

Security Strategy Model (SSM) for wireless technologies: A Security Strategy Model is a solution to a Threat Model. In computer security, the term threat modeling has two distinct, but related meanings. The first is a description of the security issues the designer cares about. This is the sense of the question, "What is the threat model for a Wireless network?" In the second sense, a threat model is a description of a set of security aspects; that is, when looking at a piece of software (or any computer system), one can define a threat model by defining a set of possible attacks to consider. It is often useful to define many separate threat models for one computer system, this way you have groups of more narrow set of possible attacks to focus on. Having a threat model you can assess the probability, the potential harm, the priority etc. of attacks, and from this point on try to minimize or eradicate the threats. The two senses derive from common military uses in the United States and the United Kingdom			
Dependent Variables	**Data Measure of Dependent Variable**	**Independent Variables**	**Data Measure of Independent Variable**
Threat Model		Possible attacks, security issues, counter measures, wireless configuration, wireless protocols, RFID waves	

Table 2: Security Strategy 'Threat Model'

The general idea of using the BS ISO/IEC 17799:2005 is so that the SSM is created based on best practice within the ICT industry of protecting confidential data or at least that the possible risks that stem from using the SSM are mitigated against; this is also known as risk based auditing. Table 3 identifies the dependent and independent variables of the ITG used in the proposed solution to validate the components of the SSM

5. Statistical analysis of the (SSM) data:

In order to obtain and analyse the correct sample data the research shall adopt the approach used for statistical studies which comprises of (Surveys, experiments, observational studies etc). This will enable a big enough effect to be of scientific significance (Lenth 2001). In contrast to this other researchers have however suggested the use of a methodology of discrete-event simulation for manufacturing systems.

This is so as to benefit from the analysis and interpretation of simulation results that come with using the model (Groumpos and Merkuryev 2002).

This model is also very useful for this research and whilst the author will not adopt the recommendations in all entireties the data collation procedures and processes shall be adopted in order to maximise the results.

In comparison other researchers have said that the rules used have to be tested not by statistical means but by validating the prohibitions, authorisations and obligations

To research the IT Governance standards for LBS: Information Technology Governance, IT Governance or ICT (Information & Communications Technology) Governance, is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. The rising interest in IT governance is partly due to compliance initiatives (e.g. Sarbanes-Oxley (USA) and Basel II (Europe)), as well as the acknowledgment that IT projects can easily get out of control and profoundly affect the performance of an organization			
Dependent Variables	**Data Measure of Dependent Variable**	**Independent Variables**	**Data Measure of Independent Variable**
Trust Model		ITIL	
		COBIT	
		ISO 27001	
		ISO/IEC 38500:2008	
		BS7799	

Table 3: Information Technology Governance (ITG) variables

which can be integrated into one by restricting predicates or by adding transitions and states (Mallouli, Orset et al. 2007). However due to the significance of this studies results and the size of the data it would not be possible to validate the data using this method

6. Methodology:

Research Approach will be by Methodological Triangulation which is a mixture of qualitative and quantitative methods of data collection

a) Sample size – large samples are often Quantitative because of the need to conduct statistical analysis
b) Theories and Hypothesis – Part of my research will study the relevant literature to establish any gaps in the literature. Whilst the other part will not use relevant literature but an experiment that will be observed for causal relationships
c) Types of data – quantitative data is highly precise and specific. Because measurement is an essential element of the research process. However under qualitative data the emphasis is quality and depth of the data. My research will use both to remove the bias of each
d) Location – quantitative research is usually carried out in the lab which is where my research is carried out. Under qualitative research the study is usually carried out in the field which is where my survey data and interview data will come from.
e) Reliability – under qualitative research it is not so important if qualitative measures are reliable. However as my research needs the credibility of being able to stand up to scrutiny. I intend to use quantitative measures to ensure my model is reliable
f) Validity – Is the extent to which the research findings actually represent what is happening in the situation. My research is quantitative because it focuses on precision measurements and the ability to be able to repeat the experiment reliably. Also qualitatively the essence is capturing

the richness of the data for explanation and analysis.

g) Generalisability – The extent to which I can come about the conclusions about one thing based on the information about another. This is because using statistics to generalise from a sample to a population is just one type of generalisation and I may be able to generalise in another

7. Conclusion:

The research is completely holistic in its approach and the security strategy model will be unique. To the best of the author's knowledge, no previous work has attempted to create a security strategy model using LBS within and outside a geographical test bed that is conditioned by wireless protected access protocols and Information Technology Governance standards. The primary contribution of the research will be the design of the security strategy model and the development of a supporting theoretical framework for the model

8. References:

Chen, Y. and Chan, Y. et al (2005). "Enabling location based services in wireless LAN hotspots." International Journal of Network Management **15**: 163-175.

Jensen, C. and Kigys, A. et al (2002). "Multidimensional Data Modelling for Location-Based Services." ACM: 55-61.

Hori, Y. and Sakurai, K (2006) 'Security Analysis of MIS Protocol on Wireless LAN comparison with IEEE802.11i' in wireless mobile networks *Mobility 06*, Oct. 25–27, 2006, Bangkok, Thailand; Pg1-5 http://delivery.acm.org/10.1145/1300000/1292344/a11-hori.pdf?key1=1292344&key2=2275225911&coll=portal&dl=ACM&CFID=832647&CFTOKEN=32574418; Accessed: 16/11/07

Ijeh, A. et al (2008); in press. Geofencing in a security strategy model in the conference proceedings of ICDIM held at the School of Computing and Technology, University of East London, UK

Lenth, R. (2001). "Some Practical Guidelines for Effective Sample-Size Determination." 1-11.

Groumpos, P. and Y. Merkuryev (2002). "A methodology of discrete-event simulation of manufacturing system: an overview."

Mallouli, W., J. Orset, et al. (2007). "A formal for testing security rules." ACM: 127-132.

Ustan, V., L. Yilmaz, et al. (2006). "A conceptual model for Agent-based Simulation of Physical Security Systems." ACM: 365-370.

Pedegraft, N., M. Rounds, et al. (2005). "A Simulation Model of IS Security." ACM: 172-177.

Sanchez, S. (2007). "Work smarter, not harder: Guidelines for designing simulation experiments." IEEE **1**.

Stubblefield, A. et al. (2004) 'A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)' in ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pg 319–332. Accessed from: http://delivery.acm.org/10.1145/1000000/996948/p319stubblefield.pdf?key1=996948&key2=3129025911&coll=portal&dl=ACM&CFID=832647&CFTOKEN=32574418; Accessed: 16/11/07