Monitoreo de la Seguridad de la Información en Redes Wifi con Detección de Fallos y Envío de Avisos de Alerta a Dispositivos Móviles Android

Ingrid Julieth Velásquez Artunduaga, Estudiante Especialización en Proyectos Informáticos[1], Andrés Ramírez Peña, Ingeniero en Telemática[2], Miguel ángel Leguizamón Páez, Magister en ciencias de la información y las comunicaciones[3]
[1, 2 y 3] Universidad Distrital Francisco José de Caldas, Colombia, ingridjulieth20@gmail.com, andramp@gmail.com, mianlepa@gmail.com

***Abstract*– The security is an aspect that is particularly relevant when it comes to wireless networks, especially because is deployed in an area and anyone can access this, then is necessary to have different security systems to increase the perceived level of confidence users of the network. Thinking about this proposes the development of a system for continuous monitoring of the network to detect security problems and then proceed to notify a mobile device the problem, in addition to track the alleged intruder and to perform an analysis of network vulnerabilities.**

I. Introducción

La irrupción de la novedosa tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas a futuro para el desarrollo de sistemas de comunicación, así como nuevos riesgos.

La flexibilidad y la facilidad de acceso a las redes inalámbricas WiFi han hecho que los gobiernos generen políticas para diversificar su uso, lo que la ha convertido en una tecnología importante de uso masivo facilitando el derecho de acceso a la información.

Las redes inalámbricas ofrecen un gran abanico de ventajas frente a las tradicionales redes cableadas, facilidad de instalación, amplia cobertura, movilidad, ampliación sencilla, entre otras; es precisamente gracias a estas características que las redes inalámbricas han tomado un gran apogeo en la actualidad.

La seguridad es un aspecto que cobra especial relevancia cuando se habla de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

La seguridad en el intercambio dela información que viaja a través de una red inalámbrica debe garantizarse, y para ello es necesario tener un sistema que la proteja brindando a sus usuarios confianza ante las posibles amenazas que se puedan presentar debido a su dispersión espacial y dote de seguridad a las comunicaciones y a las entidades que se comunican , de tal manera que si en algún momento es interceptado un paquete que está viajando a través de la red, inmediatamente se tome la acción correctiva del caso.

El uso del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad, la salida de estas ondas de radio fuera del perímetro donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la seguridad informática de las diferentes entidades que hagan uso de ésta tecnología [2].
El presente artículo pretende dar una visión global de los posibles riesgos a los que está expuesta la información que viaja sobre una red wifi con el fin de solventar las vulnerabilidades y amenazas y desarrollar una herramienta que permita detectar problemas de intrusión en la red.

II. Marco Teórico

Para la realización del prototipo para el monitoreo de la seguridad de la información en redes inalámbricas, fueron tenidos en cuenta los conceptos que a continuación se presentan; los cuales soportan las bases de desarrollo de este prototipo.

La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad [3].

Considerar aspectos de seguridad significa: conocer los riesgos, clasificarlos y protegerse de los impactos o daños de la mejor manera posible con el fin de solventar vulnerabilidades y amenazas y establecer una estrategia de respuesta a los riesgos que permita reducir la probabilidad de

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2016.1.2.076
ISBN: 978-0-98228996-9-3
ISSN: 2414-6390

ocurrencia o impacto del mismo y una reacción temprana en caso de ocurrencia.

Esto significa que en las compañías de hoy en día donde la información es considerada un activo tan valioso se debe ser consciente de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de todos, se pueden tomar medidas de protección adecuadas, para que no se pierda o dañe cada uno de los valiosos recursos.

En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

Gestión de riesgo en la seguridad informática: Es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. En su forma general contiene cuatro fases: Análisis, clasificación, reducción y control [4].

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos [5]. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros [6].

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Retos de la seguridad: La eficiente integración de los aspectos de la Seguridad Informática en el ámbito de las organizaciones sociales centroamericanas enfrenta algunos retos muy comunes que están relacionados con el funcionamiento y las características de estas. Los temas transversales no reciben la atención que merecen y muchas veces quedan completamente fuera de las consideraciones organizativas: Para todas las organizaciones y empresas, la propia Seguridad Informática no es un fin, sino un tema transversal que normalmente forma parte de la estructura interna de apoyo. Nadie vive o trabaja para su seguridad, sino la implementa para cumplir sus objetivos.

El proceso de monitoreo y evaluación, para dar seguimiento a los planes operativos está deficiente y no integrado en estos: Implementar procesos y medidas de protección, para garantizar la seguridad, no es una cosa que se hace una vez y después se olvide, sino requiere un control continuo de cumplimiento, funcionalidad y una adaptación periódica, de las medidas de protección implementadas, al entorno cambiante [7].

Amenazas y vulnerabilidades: Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño material o inmaterial sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e información, las amenazas y los consecuentes daños que pueden causar un evento exitoso [8].

La Vulnerabilidad es la debilidad de un sistema que lo hace susceptible a sufrir algún daño. Es necesario tener en cuenta estas vulnerabilidades para que los sistemas desarrollados cuenten con la capacitad de responder o reaccionar a una amenaza o de recuperarse de un daño.

ISO 27000: Es un conjunto de estándares desarrollados o en fase de desarrollo por ISO e IEC, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

III. Metodología de investigación

La metodología que se plantea para el desarrollo del proyecto fue propuesta por los autores teniendo en cuenta dos vertientes, una apuntando a la investigación y documentación y otra basada en RUP para el desarrollo del prototipo. Ésta metodología se implementa así:

A. Investigación Bibliográfica: Se realiza una investigación bibliográfica donde se detallan los diferentes tipos de ataques a los cuales están expuestas las redes WIFI como: denegación de servicio y ataques de fuerza bruta para romper la seguridad de la red como: suplantación y secuestro de sesiones, con el fin de solventar las vulnerabilidades y amenazas.

B. Investigación de Campo: Se realiza una investigación de campo con dos vertientes, una muestra el funcionamiento de una red wifi en condiciones normales y la otra pone a prueba los diferentes tipos de ataque consultados anteriormente, para esto se hace uso de la aplicación Wifislax la cual provee una serie de herramientas para realizar una auditoria completa sobre la red Wifi.

C. Investigación Exploratoria: Resulta necesario investigar las características de herramientas tales como Microsoft Network Monitor, Nagios, OpenNMS y las características actuales de los sistemas de monitoreo de redes inalámbricas WIFI.

D. Documentación de Resultados: Se documentan los resultados o conclusiones obtenidas después de realizadas las tres (3) primeras fases de la metodología.

E. Desarrollo del Prototipo: El prototipo se desarrolla con base en la metodología RUP.

F. Prueba de Campo y Recopilación de Información: Se realiza una prueba de campo con el prototipo proporcionando información sobre los resultados obtenidos con este.

G. Procesamiento de la Información: La información se debe procesar para poder obtener algunos datos estadísticos que indiquen el funcionamiento del prototipo.

IV. DESARROLLO

Se desarrolló un sistema que detecta fallas en la seguridad de la información y envía avisos de alerta a un dispositivo móvil configurado por el usuario para proteger la información y dotar de seguridad a las comunicaciones, además una vez es detectado el intruso y enviada la alerta, el administrador puede bloquear el puerto wireless del firewall de donde se conecta el raspberry pi desde el dispositivo móvil con el fin de realizar el proceso de gestión. Para lograr esto se cumplió con las tareas que se describen a continuación:

A. Se analizaron los posibles riesgos a los que está expuesta la información que viaja sobre la red wifi con el fin de solventar las vulnerabilidades y amenazas que pueden presentarse.

B. Se diseñó un sistema que permite enviar un aviso de alerta a un dispositivo móvil.

C. Se desarrolló un sistema que envía alertas cuando se están presentando ataques sobre una red wifi.

D. Se desarrolló un sistema que brinda mayor seguridad de la información que viaja a través de la red wifi basada en una evaluación de los riesgos a los que está sometida la información de la organización por medio de dispositivos móviles.

E. Se agregó al sistema un proceso para gestionar desde el dispositivo móvil realizando el bloqueo de un puerto una vez recibida la alerta de intrusión.

F. Se realizaron las pruebas correspondientes para confirmar el correcto funcionamiento de la solución.

Mediante los siguientes roles y actividades asociadas a estos se buscó cumplir con la metodología propuesta para la vertiente de desarrollo del prototipo:

Roles

1. Analista
2. Analista telemático
3. Arquitecto
4. Programador
5. Analista de pruebas

Actividades

1. Analista: Identificar los requerimientos y realizar un análisis de los requerimientos.
2. Analista telemático: Realizar un análisis sobre la mejor forma de afrontar los requerimientos de seguimiento y detección de intrusos y presentar un listado de soluciones que se ajustan a los requerimientos presentados.
3. Arquitecto: Realizar un análisis de la arquitectura más adecuada para el desarrollo de la solución
4. Programador: Realizar las tareas desarrollo que surjan del análisis elaborado por el analista telemático y el arquitecto, desarrollar el sistema de administración de la solución y ajustar la solución según los resultados de las pruebas.
5. Analista de pruebas: Realizar un análisis de las pruebas que se deben hacer sobre la implementación y presentar un resumen de los resultados obtenidos de las fases de pruebas.

Artefactos

1. Documento de requerimientos
2. Especificaciones de caso de uso
3. Documento de arquitectura
4. Reporte de aplicaciones desarrolladas que pueden ayudar a la solución
5. Entregables del desarrollo
6. Documento de análisis de pruebas
7. Informe resultados de pruebas

En la fase de implementación se documentaron los parámetros de la codificación, por medio de un diagrama de componentes, como en las Fig.1 y Fig. 2 en el cual se ilustran y describen detalladamente las aplicaciones utilizadas tanto para el desarrollo de escritorio como para el desarrollo móvil, así mismo se asesora con sencillos manuales su instalación.

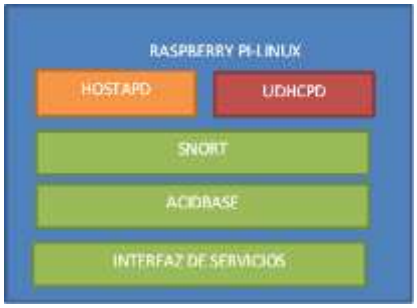

Figura. 1. Diagrama de componentes, Elaboración Propia

Figura. 2. Interfaz de servicios, aplicación android, Elaboración Propia

Dónde:

Hostapd: Es una aplicación libre para Linux encargada de convertir el sistema operativo en un acces point wifi con el uso de encriptación, claves, entre otros.

Udhcp: Es un servidor dhcp libre para Linux.

Snort: Es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL.

AcidBase: Es una aplicación php que se encarga de analizar la información recolectada en la base de datos mysql por parte de snort.

Interfaz de Servicios: Esta es una interfaz creada para proveer servicios web que consuman la base de datos de snort y envía la información al dispositivo móvil.

En la fase de calidad se incluyó el resultado de cada una de las pruebas haciendo una descripción específica de los programas de infiltración utilizados para la misma y su respectiva instalación.

Ambiente De Pruebas:

Las pruebas se realizaron en un espacio de 6x12 a diferentes distancias y con hasta 4 muros de separación entre el objetivo y el atacante. Los 10 equipos conectados en el sitio donde se realizaron las pruebas y el servidor wifi cuentan con las siguientes especificaciones:

Características Servidor WIFI	**Características Equipos Conectados**
CPU ARM 1.2Ghz Quad Core 64 bit	Portátil lenovo tarjeta wifi 54 Mbps, S.O. Ubuntu linux
1 GB Memoria RAM	Portátil hp, tarjeta wifi 54 Mbps S.O. Windows 10
Tarjeta Wifi broadcom 802.11n con soporte AP	Portátil toshiba, tarjeta wifi 54 Mbps S.O. Windows 7
S.O. Debian 8.4 (Raspbian	Portátil toshiba, tarjeta wifi 54 Mbps S.O. Windows 7
	Pc escritorio, tarjeta wifi 54Mbps S.O. Windows 10
	Tablet 7", tarjeta wifi 54 Mbps S.O. Android 5.1
	Celular Moto X, tarjeta wifi 54 Mbps S.O. Android 5.1
	Celular Iphone 4S, tarjeta wifi 54 Mbps S.O. IOS 9.3
	Celular Moto G, tarjeta wifi 54 Mbps S.O. Android 5.1
	Xbox 360, tarjeta wifi 54 Mbps S.O. Live

Para realizar las pruebas se hizo uso de las herramientas wifislax y nmap descritas a continuación: Wifislax es una distribución GNU/Linux en formato *.iso con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. WiFiSlax incluye una larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos escáner de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers y herramientas para la auditoría wireless, además de añadir una serie de útiles lanzadores.

NMAP es una herramienta para descubrir los puertos abiertos de una PC, laptop, teléfono o inclusive un router apenas especificando su dirección IP.
Esta misma herramienta permite, además, detectar las IPs de las PCs, laptops, teléfonos, routers o cualquier otra cosa que se haya conectado a la red.

Evidencia de las pruebas realizadas: Por debajo de 20 db de intensidad de señal no se pudieron realizar pruebas ya que los paquetes capturados no eran los suficientes para realizar una infiltración.

Monitorear la red específica con wifislax.

Se realizó el monitoreo de todas las redes WiFi disponibles en el área donde nos encontramos, a través de esta aplicación podemos conocer los siguientes parámetros de cada red: beacons "Indican la fuerza de la señal", BSSID que es la dirección física del dispositivo, ESSID que es el nombre que identifica a la red y el protocolo de seguridad para el acceso a la red. A mayor cantidad en beacons más posibilidades existen de poder interceptar paquetes para obtener la llave para descifrar la clave a través de diccionarios. Ver Figura. 3

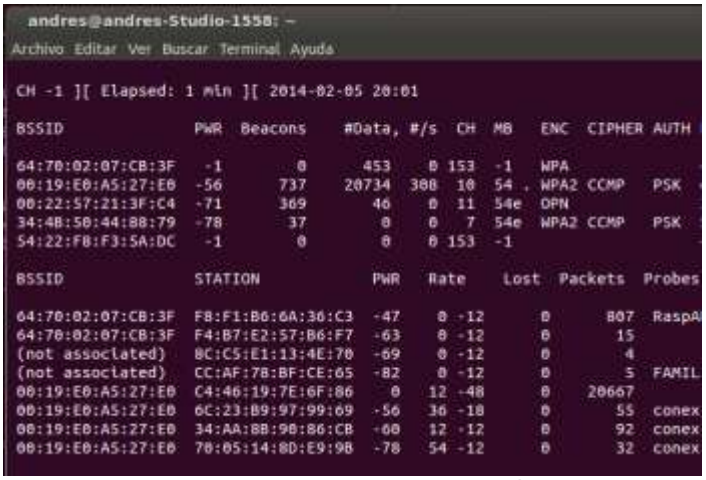

Figura. 3. Monitoreo redes Disponibles. Elaboración Propia

Podemos especificar una red para escanear y en ella encontrar cada uno de los dispositivos conectados detallando la dirección de red física de cada uno así como el número de paquetes transmitidos y el número de paquetes perdidos, también se puede verificar el nivel de señal de cada dispositivo. Analizando los paquetes que pasan entre el host WiFi y uno de los equipos conectados se puede obtener la clave precompartida y mediante un diccionario se puede llegar a conocer la clave de la red. Ver Figura. 4

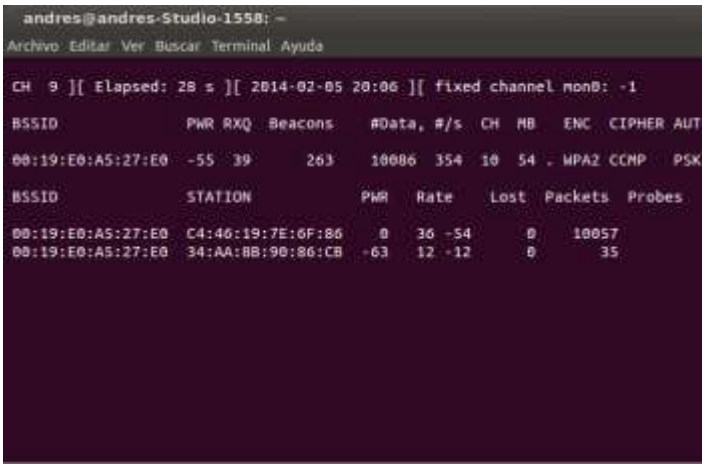

Figura. 4. Monitoreo de red específica, Elaboración Propia

Con la aplicación NMAP se puede realizar un escaneo a los puertos de un equipo específico para poder identificar qué servicios corren sobre el mismo, con esto se puede obtener la siguiente información: Número del puerto abierto, el protocolo y la aplicación que está haciendo uso del mismo. Con esta información un atacante puede conocer que tiene instalado un servidor y las vulnerabilidades que pueden ser aprovechadas. Ver Figura. 5

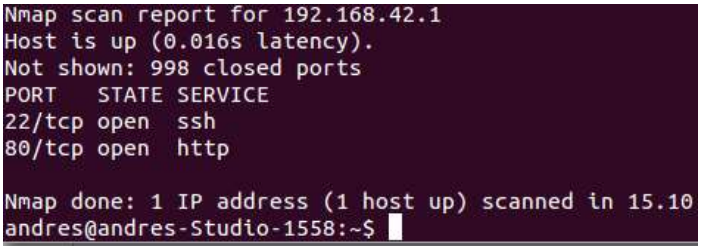

Figura. 5. Escaneo de Puertos, Elaboración Propia

El sistema debe conocer el funcionamiento de la red en condiciones normales y mediante el análisis de paquetes debe ser capaz de identificar actividad anormal sobre la misma provocada por las actividades descritas anteriormente, en ese momento enviara una alerta a un celular registrado(Ver Figura 6), quien podrá en el momento realizar una simple gestión como el bloqueo de la ip involucrada en el ataque. Posteriormente se registrara en el histórico de incidentes la información del ataque que incluye la fecha y hora del suceso, una descripción del tipo de ataque, la dirección ip donde se origina el ataque y la dirección ip atacada y el protocolo involucrado. Ver Figuras. 7 y 8

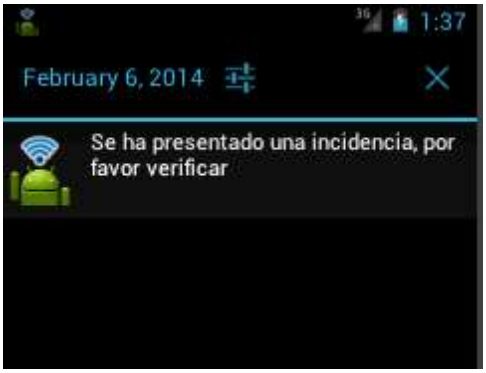

Figura. 6. Alerta en dispositivo móvil, Elaboración Propia

ID	Descripcion	Fecha
1417	SNMP Agent X Request	2014-02-15 13:25
1417	SNMP Request TCP	2014-02-20 10:42

Figura. 7. Historial de Ataques, Elaboración Propia

Direccion de Origen	Direccion de Destino	Protocolo
192.168.42.178	192.168.42.1	TCP
192.168.42.178	192.168.42.1	TCP

Figura. 8. Historial de Ataques, Elaboración Propia

V. RESULTADOS

Se desarrolló un sistema que detecta fallas en la seguridad de la información y envía avisos de alerta a un dispositivo móvil configurado por el usuario para proteger la información y dotar de seguridad a las comunicaciones. Con los siguientes alcances y limitaciones:

Alcances

A. El sistema permite monitorear la seguridad de redes wifi a través de dispositivos móviles que cuenten con la aplicación desarrollada

B. Se dispone de una aplicación web para la configuración de los dispositivos móviles que recibirán las alertas.

C. El sistema permite llevar un histórico de los problemas de seguridad presentados en redes wifi, este histórico contiene información del suceso e información de la vulnerabilidad detectada.

Delimitaciones

A. El sistema únicamente notifica problemas de intrusión.

B. La aplicación para dispositivo móvil solo corre en sistemas operativos android en sus versiones 4.2 e adelante hasta la 5.1 que es la actual.

C. Se debe disponer de una conexión a la red o a internet para poder recibir las notificaciones de seguridad.

VI. CONCLUSIONES Y TRABAJOS FUTUROS

Se analizaron los posibles riesgos a los que está expuesta la información que viaja sobre una red wifi y cómo solventar las vulnerabilidades aportando soluciones ante las posibles amenazas a la información que viaja sobre las redes inalámbricas realizando la planeación de la gestión de riesgos haciendo uso y comprendiendo la herramienta magerit.

Esta herramienta tecnológica detecta fallas en la seguridad de la información en redes wifi y envía avisos de alerta a un dispositivo móvil cuando se están presentando ataques sobre la red. Este sistema brinda mayor seguridad de la información que viaja a través de la red wifi basada en una evaluación de los riesgos a los que está sometida la información de la organización por medio de dispositivos móviles.

Se evidencia que para realizar un ataque en una red wifi es necesario que esa red esté conectada a un equipo y además que esté generando tráfico sobre ella. El configurar las aplicaciones de monitoreo para que la detección sea más certera puede ocasionar lentitud en la red.

El tema de seguridad de la información en redes inalámbricas es bastante amplio; el proyecto se centra únicamente en problemas de intrusión, por lo tanto se sugiere escalarlo poco a poco con el fin de solventar la mayoría de vulnerabilidades que puedan presentarse.

Las alertas que se generan en el dispositivo móvil se presentan cuando se está realizando un intento de infiltración con aircrack-ng, cuando se realiza un mapeo de puertos o cuando se realiza un ataque de denegación de servicio, se sugiere para mejorar el prototipo ampliar el proceso de pruebas que permitan generar más mensajes de alerta con las especificaciones pertinentes.

VII. REFERENCIAS

[1] D. A. Allal, R. Weber, I. Cognard, G. Desvignes and G. Theureau, "RFI mitigation in the context of pulsar coherent de-dispersion at the Nancay Radio Astronomical Observatory," Signal Processing Conference, 2009 17th European, Glasgow, 2009, pp. 2052-2056. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7077659&isnumber=7077262

[2] G. Betarte and M. E. Corti, "Design and implementation of a computer security Diploma," Computing Conference (CLEI), 2013 XXXIX Latin American, Naiguata, 2013, pp. 1-6. doi: 10.1109/CLEI.2013.6670620 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6670620&isnumber=6670594

[3] E. Amankwa, M. Loock and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for, London, 2014, pp. 248-252. doi: 10.1109/ICITST.2014.7038814URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7038814&isnumber=7038754

[4] R. Bista, H. K. Yoo and J. W. Chang, "A New Sensitive Data Aggregation Scheme for Protecting Integrity in Wireless Sensor Networks," Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, Bradford, 2010, pp. 2463-2470. doi: 10.1109/CIT.2010.422 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5578283&isnumber=5577816

[5] A.P. Jardosh, K.N. Ramachandran, K.C. Almeroth and E.M. Belding-Royer "Understanding Congestion in IEEE 802.11b Wireless Networks" Proc. ACM SIGCOMM

[6] Albrechtsen, E. & Hovden, J., 2009. The information security digital divide between information security managers and users. Computers & Security, 28(6), pp. 476-490.

[7] Wolf, M., Haworth, D. & Pietron, L., 2011. Measuring an information security awareness program. Review of Business Information Systems - Third Quarter, 15(3), pp. 9-22.

[8] Laudon, C.K., & Laudon, P.J., 2010. Management information systems. New Jersey: Prentice Hall.

[9] Da Veiga, A. & Eloff, J.H.P., 2010. A framework and assessment instrument for information security culture. Computers & Security, 29(2), pp. 196-207.

[10] Rezgui, Y. & Marks, A., 2008. Information security awareness in higher education: An exploratory study. Computers & Security, 27(7-8), pp. 241-253.