Voto electrónico con SSL/TLS e IPSEC

Electronic voting with SSL / TLS and IPSEC

Raúl Bareño Gutiérrez, Omar Lengerke

Abstract— **Colombia is currently debating the implementation of electronic voting; fears exist in the transmission of data. The research reviews the potential vulnerabilities in the transmission to common computer attacks on data centers. This E-vote protects prototype he sent giving reliability and transmission reliability. The (E-VOTE) tool using the SSL / TLS protocols are used for authentication of the voter via WEB site and validates the data and IPSEC protocol protecting certain communications to external attacks and unauthorized transactions to ensure authentication, integrity and besides confidentiality and anonymity of the voter polling stations. Electronic voting in Colombia based on this prototype is unsure whether additional security measures for the transport and handling of data and protocols such as SSL / TLS are implemented supplemented with IPSEC can be used for transmission to the data centers.**

Index Terms —Electronic voting, IPSEC, SSL / TLS. Security Protocols.

I. INTRODUCCION

Hoy el voto electrónico intenta disminuir algunas vulnerabilidades del sistema tradicional, Colombia debate el uso o la inclusión de nuevas tecnologías de la información tic [1] en las votaciones presentándose dudas en la transmisión de los datos a pesar que ya ha adelantado planes piloto en algunas regiones [2]. Con el uso de las tic se hace fácil, sencillo y seguro la implementación del sistema electrónico de votación. En la actualidad países y universidades en grecia, noruega, méxico, españa, argentina [3] entre otros, usan e investigan la implementación de sistemas de envió de datos seguros que permiten garantizar las características del voto universal en cuanto a unicidad, secreto, autenticación, libertad de acceso y de elección entre otros. Países donde ya se aplica el voto electrónico presencial como australia, bélgica, brasil, canadá, estonia, francia, alemania, india, italia, holanda, noruega, suiza, reino unido, venezuela, paraguay, argentina. Y más de 30 países con exitosa aplicación sobre todo en la fase de transmisión unos utilizan protocolos como ssl/tls y otros ipsec de formas independientes y no integradas al sistema de votación mismo.

Raúl Bareño Gutiérrez, docente tiempo completo Corporación Universitaria Minuto de Dios (Uniminuto). Bogotá Colombia, raul.bareno@uniminuto.edu

Omar Lengerke, Secretario de Tecnologías de la Información y las Comunicaciones SETIC, Gobernación de Santander, Colombia, profesor Titular Unab. Colombia, olengerke@unab.edu.co

IPSEC: Es un conjunto de estándares sus servicios basados en criptografía utilizado para cifrar datos para que no se puedan leer o manipular durante su viaje a través de una red IP. Puede utilizarse en ipv4 o ipv6 [6], opera en la capa de red (del modelo osi), Permitiendo privacidad y autentificación máxima de los datos. Ofrece tres funcionalidades: Una de autentificación con (ah) [7]. Otra mixta de autentificación/encriptamiento (esp) [8]. La última de intercambio de llaves por el protocolo de gestión de claves (ike) [9], [10]. Funciona de dos formas: en modo transporte o modo túnel [8]. En el modo transporte la seguridad se aplica sólo a las capas más altas de los datos [11]; En modo túnel tanto los datos de los protocolos de las capas superiores como el encabezado IP del paquete son protegidos a través del encapsulamiento.

En cuanto al protocolo SSL (secure sockets layer capa de sockets seguro) [12]. Desarrollado por netscape el objetivo es proveer privacidad y confiabilidad a la comunicación entre aplicaciones cliente servidor vía web para autenticar los equipos. Tls surge de la necesidad de estandarizar un protocolo que provea seguridad entre el cliente y el servidor a través de internet debido a que ssl es un protocolo creado y patentado por netscape y una evolución del protocolo ssl el cual establece una conexión segura por medio de un canal cifrado entre el cliente y el servidor [13]. Ssl/tls es un protocolo de seguridad en navegadores web y servidores para ayudar a los usuarios a proteger sus datos mientras se transfieren [14]. Las características de Ssl/Tls son: seguridad criptográfica, interoperabilidad, extensibilidad, eficiencia. Trabaja arriba de la capa de transporte y entre las aplicaciones a nivel web [15].

Esta investigación revisa el uso y funcionamiento de la tecnología para procesos de votación electrónica bajo ambientes tic, la herramienta desarrollada integra en un solo sistema parámetros de seguridad mediante los protocolos ssl/tls protegiendo el aplicativo en la capa de aplicación y además lo protege en la capa de red y de transporte del modelo osi [4] con el protocolo ipsec a lo hora de transmitir los datos que entrelazados le aportan seguridad al sistema para el caso Colombiano, además contrarrestan ataques informáticos comunes como dos, ddos y hombre en el medio (mitm) por citar los más referentes. Este prototipo con estos protocolos evita la manipulación de la información durante la transmisión hacia diferentes centros de cómputo internos o externos aportando autenticación, integridad y confidencialidad a los electores como a los datos.

II. MATERIALES Y METODOS

Los protocolos ipsec, ssl/tls operan durante la transmisión de la información básica del elector y jurado en el prototipo E-vote [5] y en el posterior envió de los resultados.

En cuento al procedimiento de instalación del prototipo E-vote se hizo en un escenario así:

- Instalación de los periféricos: lector de código de barras [16] y de huella dactilar [17] en un pc.
- Instalación del servidor web con la base de datos mysql y los protocolos ssl/tls e ipsec bajo el sistema operativo Linux, con arquitectura a nivel de dispositivos activos como routers, switches (Ver Fig. 3).

Se efectuó la simulación para 3 escenarios controlados así:

1. En una intranet.
2. En una extranet.
3. Los dos protocolos ssl/tls e ipsec en un sistema integrado.

Los ataques escogidos fueron:

- Denegación de servicio (dos)
- Denegación de servicio distribuido (ddos) [18].
- Hombre en el medio (mitm) [19].

Las pruebas para él envió del archivo en los escenarios 1 y 2 son:

Prueba 1: envió con seguridad ssl/tls, sin ataques.
Prueba 2: envió con seguridad ssl/tls, con ataques (dos).
Prueba 3: envió con seguridad ssl/tls, con ataques (ddos).
Prueba 4: envió con seguridad ssl/tls, con ataques. (Mitm).
Prueba 5: envió con seguridad ipsec, sin ataques.
Prueba 6: envió con seguridad ipsec, con ataques (dos).
Prueba 7: envió con seguridad ipsec, con ataques (ddos).
Prueba 8: envió con seguridad ipsec, con ataques (mitm).

En el escenario 3 se transmitió con seguridad ssl/tls e ipsec sin ataques debido a los mecanismos de seguridad que tienen estos protocolos no se puede hacer ningún tipo de ataque de los analizados en este proyecto.

El procedimiento efectuado fue el siguiente:

Paso 1: el elector se reporta en la mesa de votación con su documento de identificación con hologramas, el sistema valida el documento verificando los campos nombres, apellidos y numero de cedula con los registrados previamente.

Paso 2: Una el sistema valida las fases previas de autenticidad y son superadas con éxito por parte del elector se activa el prototipo electrónico y la persona queda lista y apta para votar; igual procedimiento para él envió del archivo. En cuanto a la transmisión de los datos hacia los centros de cómputo ubicados en la intranet o extranet, el sistema utiliza los dos protocolos ssl/tls para la validación de los datos en el prototipo e ipsec para la transferencia de archivos en la capa de red. (Fig. 1).

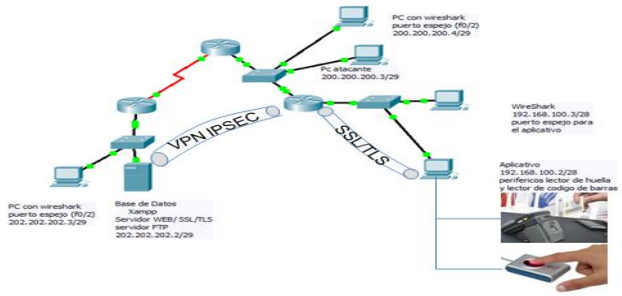

Figura 1. Transmisión de los datos.

III. RESULTADOS

Para facilitar el análisis de resultados se consideran las variables así:

- Tiempo de envió
- Paquetes enviados por el aplicativo (PC1)
- Paquetes recibidos por la BD
- Bytes enviados por PC1
- Bytes recibidos por la BD
- % de ocupación del canal PC1
- % de ocupación del canal BD
- % de procesamiento PC1
- % de procesamiento BD
- % de disponibilidad del canal
- Archivos enviados
- Numero de atacantes.

Las pruebas efectuadas se hicieron enviando entre uno y tres archivos por 10 veces por escenario, los atacantes estuvieron entre 1 y 10 y el tamaño del archivo .PDF enviado era de 21 Kbyte, como máximo.

3.1 Pruebas y análisis para el escenario 1 intranet.

Para esta prueba en el escenario 1 (ver fig. 2) se hizo el montaje controlado a nivel de infraestructura de telecomunicaciones configurando los switches, la base de datos y los pc para poder efectuar el análisis de trafico respectivo y revisar las diferentes variables consideradas en el proyecto (ver tabla I) se tabularon de acuerdo a sus promedios arrojando los siguientes resultados:

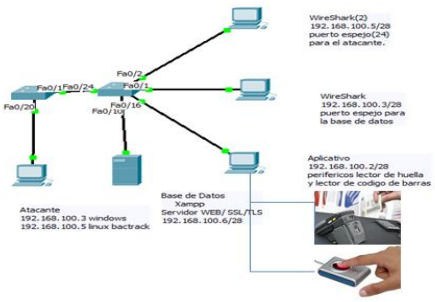

Figura 2. Escenario 1 intranet.

Tabla I

Escenario 1 Intranet

Escenario 1	DoS	DDoS	MITM	Sin Ataques
Tiempo. envió	30	29	33	26
Paquetes. Enviados pc1	149	150	118	114
Paquetes Recibidos bd	231496	285678	127	114
Bytes pc1	30403	34416	54618	52070
Bytes bd	2190620	7906355	58512	53298
% ocupa canal pc1	1,1	2	1	2
% ocupa canal bd	77	92,5	2	2
% proce pc1	2,1	3,9	4,3	5,2
% proce bd	85,6	94,1	4,8	6,1
% disponi del canal	23,1	7,5	98,5	97,70
Archivos	1,2,3	1,2,3	1,2,3	1,2,3
Atacantes	1,5,10	1,5,10	1,5,10	1,5,10

Fuente: Autor.

Se revisaron los paquetes recibidos en la base de datos durante los ataques de dos y ddos efectivamente se incrementan con relación a los enviados por el aplicativo (ver Fig. 3); Provocando aumento en el procesamiento de la base de datos y limitando el ancho de banda del canal de manera significativa (ver Fig. 4). Además si el mantiene el ataque por más de 5 minutos continuos congestiona el canal al punto de deshabilitar el servicio de votación y de envió.

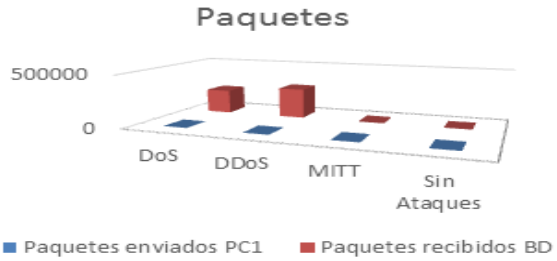

Figura 3. Cantidad de paquetes

Durante los cortos tiempos de envió a pesar de los ataques el servicio se mantiene, y permitiéndole la llegada al destino sin ningún inconveniente.

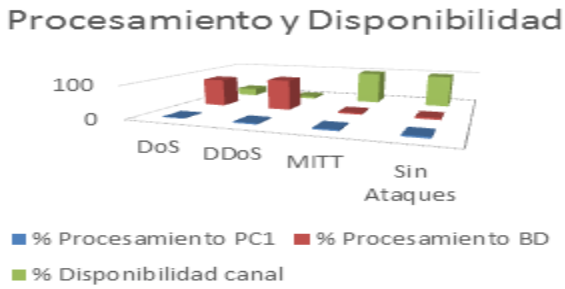

Figura. 4. Procesamiento y disponibilidad del canal

Debido al alto consumo de ancho de banda de los ataques el porcentaje de disponibilidad del canal en dos de 23,1% y en ddos de 7,5%.

Para el ataque de mitm se visualiza el tráfico capturado pero viaja con el servicio tls/ssl con cierto grado de seguridad (Ver Fig. 5). Se nota claramente los algoritmos de autenticación y confidencialidad con los que opera dicho protocolo pero no puede desencriptar la información.

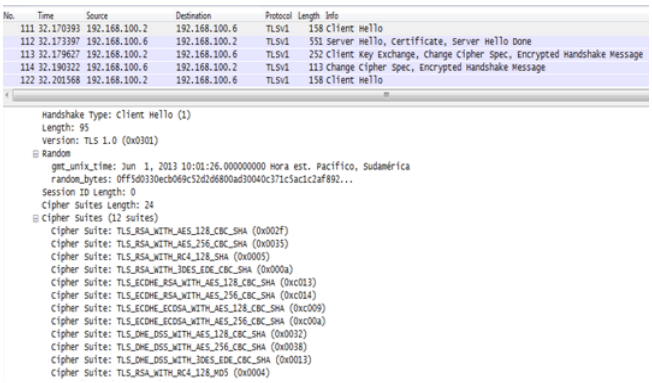

Figura 5. Trafico con TLS/SSL

3.2 Pruebas y análisis para el escenario 2 extranet con ssl/tls.

Bajo este escenario (ver fig. 6) se amplió el radio de acción y se hizo el montaje a nivel de infraestructura de telecomunicaciones configurando ahora routers, switches, la base de datos y los pc para poder efectuar el análisis de trafico respectivo y revisando las mismas variables del proyecto bajo el protocolo ssl/tls (ver tabla II) se tabularon de acuerdo a sus promedios arrojando los siguientes resultados:

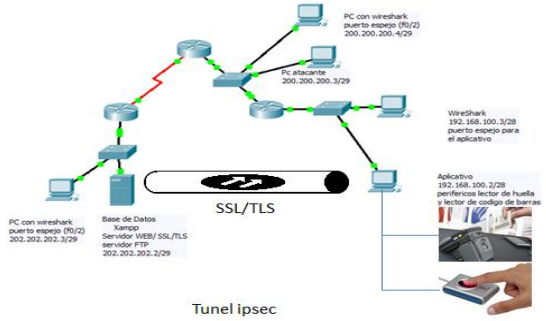

Figura 6. Escenario 2 extranet con ssl/tls.

Tabla II

Extranet con SSL/TLS

Esc 2 extranet con SSL/TLS	DoS	DDoS	MITM	Sin Ataques
Tiempo envió	26	30	29	36
Paquetes enviados pc1	239	239	168	239
paquetes recibidos bd	72876	122059	176	245
Bytes pc1	62385	62385	73045	62385
Bytes bd	3929692	4028534	76201	63889
% ocupa canal pc1	0,0259	0,0259	0,0188	0,0227
% ocupa canal bd	66,1	86	0,0193	0,021
% proce pc1	1,9	1,9	4,4	2,9
% proce bd	68,5	68,1	4,8	4,1
% disponi del canal	33,9	14	99,98	99,98
Archivos	1,2,3	1,2,3	1,2,3	1,2,3
Atacantes	1,5,10	1,5,10	1,5,10	1,5,10

Fuente: Autor.

En esta prueba los datos viajan mayor distancia entre los dos puntos el tamaño de los paquetes aumentan en relación con los enviados debido a los ataques (ver fig. 7) se resalta la continuidad del servicio de votación aunque lento garantiza él envió de los datos.

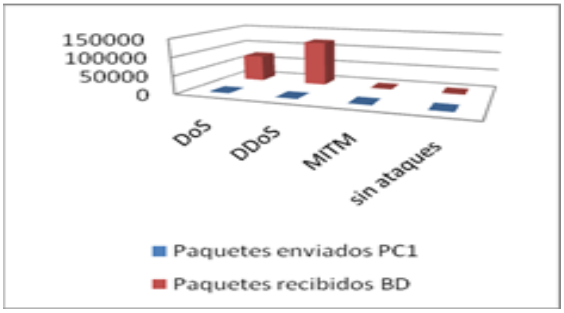

Figura 7. Cantidad de paquetes

El porcentaje de procesamiento en la base de datos aumenta y disminuye la disponibilidad del canal para dos a 33,9%, para ddos a 14%, y para el ataque de hombre en el medio a 99,98%. (Ver tabla II y Fig. 8). En esta prueba se mantuvo el ataque por más de 7 minutos para el ataque de ddos hasta que el canal y el procesamiento de la base de datos se saturan y se cae el servicio.

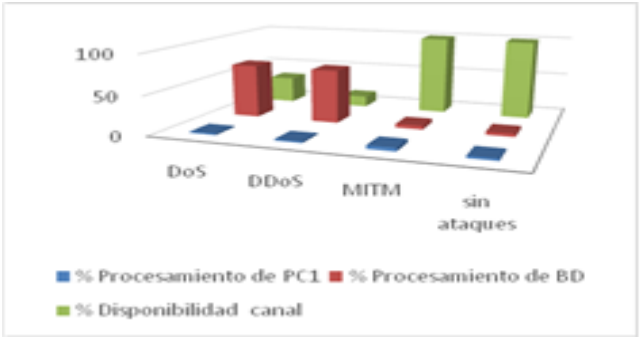

Figura 8. Procesamiento y disponibilidad del canal

3.3 Pruebas y análisis para el escenario 2 extranet con ipsec

En este escenario (ver fig. 9) se cambió la configuración de los routers con sistemas operativos seguros creándose una vpn con mecanismos de autenticación y encriptamiento fuertes como listas de control de acceso y sistemas de encriptamiento propios del protocolo ipsec como ah, también los switches, la base de datos y los pc, para efectuar el análisis de trafico respectivo revisando las mismas variables del proyecto bajo el protocolo ipsec (ver tabla III) se tabularon de acuerdo a sus promedios arrojando los siguientes resultados:

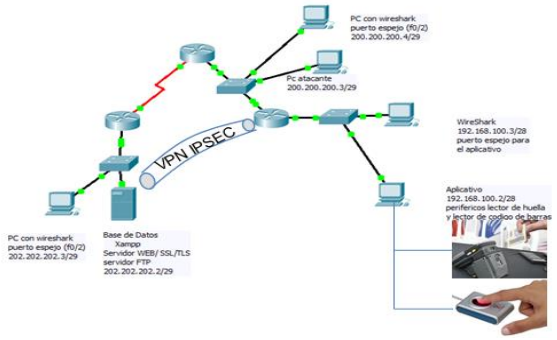

Figura 9. Escenario 2 extranet con ipsec

Tabla III

Escenario 3 con IPSEC

escenario 3 con IPSEC	DoS	DDoS	MITM	Sin Ataques
Tiempo envió	22	24	31	35
Paquetes enviados pc1	270	282	263	239
Paquetes recibidos bd	86675	86674	272	245
Bytes pc1	62385	63841	66559	62385
Bytes bd	4096875	4377308	80620	63889
% ocupa del canal pc1	0,0402	0,0402	0,0188	0,0227
% ocupa	72,3	74,3	0,0193	0,021

canal bd				
% proce pc1	4,4	4,4	4,4	2,9
% proce bd	74,9	75,4	4,8	4,1
% dispo del canal	27,7	25,7	99,98	99,98
Archivos	1,2,3	1,2,3	1,2,3	1,2,3
Atacantes	1,5,10	1,5,10	1,5,10	1,5,10

Fuente: Autor

Durante esta prueba se crea un túnel entre los dos puntos ubicando el atacante dentro de la trayectoria del túnel congestionando y limitando la disponibilidad del canal para dos a 27,7% para ddos a 25,7% y para hombre en el medio a 99,98%. (Ver Fig. 10).

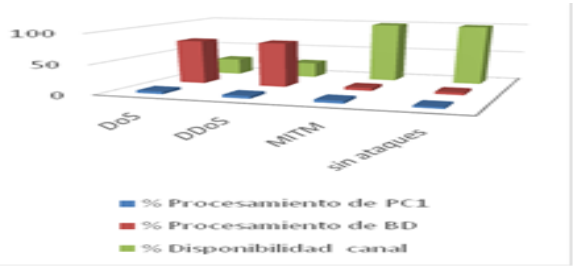

Figura 10. procesamiento y disponibilidad del canal

Otra prueba fue ubicar el atacante fuera de la trayectoria del túnel pero dentro del sistema mismo aquí ya no puede congestionar ni el canal ni el procesamiento de la base de datos porque no lo ve. Al capturar tráfico solo se visualiza las direcciones IP de las entradas del túnel (ver Fig. 11) a pesar que logre identificar las direcciones IP de los extremos e intenta hacer el ataque de dos y ddos buscando la caída del canal por congestión y limitando la disponibilidad del canal al punto que 8 minutos después mantener el ataque de manera continua logra la caída del enlace.

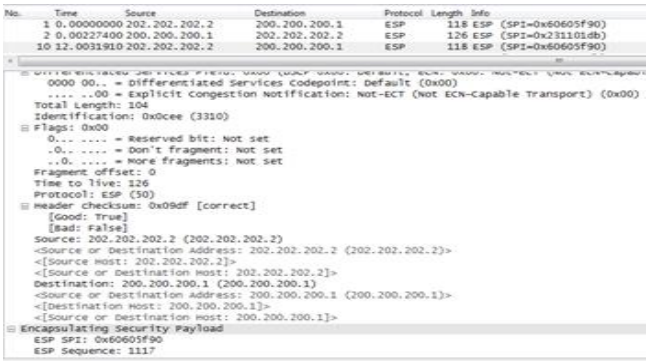

Figura 11. Visualización túnel

Para el ataque de hombre en el medio solo visualiza el tunel ahora el protocolo ipsec le ofrece mejores garantias de seguridad porque no se conocen las direcciones IP de origen y destino, ademas el tunel esta formado por el protocolo esp que encapsula tanto las IP como los datos mismos en un nuevo encapsulado.

Solución propuesta: (ver Fig. 1 y tabla IV) se crea un nuevo escenario con politicas de seguridad y mejores condiciones comparandola con los anteriores asi:

Tabla IV

Comparativo por Escenarios

Escenario Propuesto	Escenario 1 TLS	Escenario 2 TLS	Escenario 2 IPSEC	Escenario 3 TLS e IPSEC
Tiempo	26	35	20	38
Paquetes enviados PC1	114	239	263	290
Paquetes Recibidos BD	114	245	255	297
% Ocupa del canal PC1	2,4	1,227	1,227	2,3124
% Ocupa del canal BD	2,3	1,021	1,021	3,7
% Proce en PC1	5,2	2,9	5,1	8
% Proce en BD	6,1	4,1	6,4	6
% Dispo del canal	97,7	99,977	99,97	96,3

Fuente: autor.

En esta propuesta ya no se valoran los escenarios con los ataques porque es dificil que el atacante conozca los criterios basicos para hacerlo como: no conocer las IP de origen y destino de los dispositivos, el tunel se crea entre los dos es decir entre el dispositivo de la base de datos y PC donde esta instalado el prototipo E-vote a pesar que pueda capturar el trafico y conocer las IP de origen y destino del tunel y mediante politicas de seguridad configuradas en los dispositivos intermedios como los routers y los switches no tiene interconexion con los mismos a pesar que se encuentre dentro de la trayectoria y pueda capturar el trafico solo visualiza el tunel. Esto garantiza fiabilidad en la transmisión con politicas de autenticación, confidencialidad e integridad entre los dos puntos utilizando protocolos ssl/tls con sus algoritmos de seguridad desde el aplicativo hasta el dispositivo intermedio en un extremo y desde el router de borde que atravieza internet con ipsec garantizando la entrega de la información de manera segura a la base de datos o servidor principal.

Efectuando el comparativo de los escenarios cuando se envia la información con ssl/tls e ipsec se envian mas paquetes (ver Fig. 12) que los otros escenarios esto se da por las politicas de encapsulamiento que utilizan los algoritmos de seguridad que operan entre los dos dispositivos.

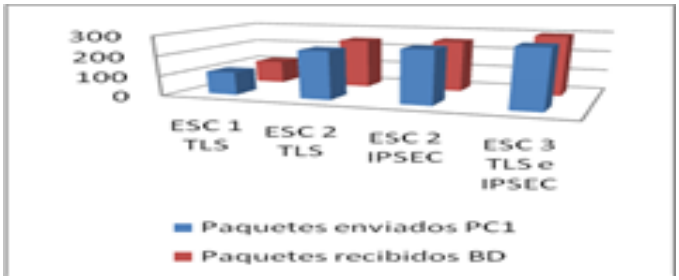

Figura 12. Paquetes Enviados

En cuanto a la ocupación del canal durante el envio de datos no es significativo usando los dos protocolos de seguridad el consumo de ancho de banda disponible es del 96,3% (ver Fig. 13).

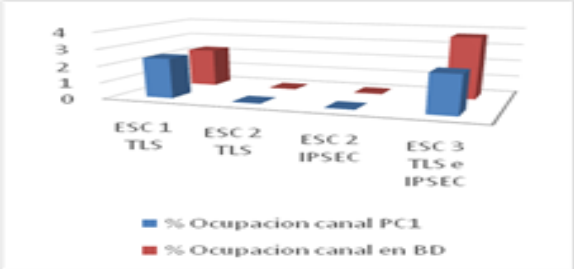

Figura 13. Ocupación del canal

IV. DISCUSIÓN

Son muchos los análisis y proyectos acerca del voto electrónico en américa latina específicamente para el caso colombiano [20]. Venezuela, brasil, paraguay y perú [21] que a pesar de su barreras en términos de acceso a internet y a las tic lo aplica y prueba en algunas regiones. Por ello los protocolos ipsec y ssl/tls fortalecen la transmisión de los datos en caso de implementarse el voto electrónico en Colombia integrados en un solo sistema, en otros países estos protocolos garantizan él envió de información [22] de manera aislada entre los diferentes puestos de votación y los data center independientemente. Por lo cual nos lleva a revisar las características específicas de cada protocolo así: (Ver tabla V).

Tabla V

Características de SSL/TLS e IPSEC para el prototipo E-vote

SSL/TLS	IPSEC
Es específico para la aplicación, opera en la capa intermedia entre tcp y http.	Protege todo el tráfico IP entre el equipo, es operativo en la capa de red
Se puede elegir si se desea ssl/Tls en cada conexión (desde la aplicación del cliente).	Es una configuración general del equipo y no admite el cifrado de conexión de red especifica
Vinculado a la aplicación E-vote	Es transparente para el E-vote y por lo tanto puede utilizarse con protocolos seguros que se ejecutan sobre IP
La implementación depende de la facilidad que la aplicación presente	Es complejo de implementar
Su implementación es transparente para el usuario	Su implementación no es transparente para el usuario
Usa tecnología embebida en los navegadores web	Solución propietaria con vpn cliente se necesita instalar software adicional
Se aplica en el modelo cliente/servidor	Es usada para unir los puestos de votación a los centros de cómputo.
No requiere software adicional, pero no da seguridad en el pc de origen y destino	Se requiere configuración adicional del firewall, pero no da mejor control en la seguridad del pc de origen o destino
Proporciona cifrado fuerte	Proporciona un fuerte encriptamiento y protege la integridad
Solo protege comunicaciones basadas en tcp.	Solo protege comunicaciones basadas en IP.
Se usa para autenticar el servidor al cliente, pero no el cliente al servidor	No protege las comunicaciones entre los pc y la puerta de enlace

Fuente: Autor

Es evidente que en el futuro habrá más necesidad de contar con redes de telecomunicaciones seguras, y ssl/tls en cuanto a universalidad no en calidad es fuerte en estos campos de enviar información cifrada por canales inseguros. Fácil será pensar que en el terreno de las comunicaciones seguras sea desplazado en algún momento por ipsec sobre todo en el terreno específico de las aplicaciones de comercio electrónico y de E-vote [6]. Por el momento ssl/tls e ipsec son muy funcionales si se quiere utilizar para aplicaciones específicas como el voto electrónico. Asociándose en tres grupos: los que son más restrictivos que ssl en cuanto a posibles aplicaciones (Como s-http), los que no aportan nada nuevo a lo que ya hace bien ssl/tls y los que aportando mejores mecanismos y más seguridad se ven desfavorecidos por su mayor coste de implementación y mantenimiento como ipsec.

V. CONCLUSIONES

La seguridad en sistemas de votación electrónico son indispensables a la hora de transmitir por redes públicas hoy se aprovechan las nuevas posibilidades que ofrecen las redes telemáticas para el fortalecimiento transparencia y confianza a estos sistemas debido a que usuarios maliciosos pueden

escuchar fácilmente el tráfico redirigirlo, introducir paquetes falsos, modificar paquetes, montar ataques de denegación de servicio (DoS), denegación de servicio distribuido (DDoS) o de hombre en el medio (MITM). Por ello se fortalecen los procesos electorales que introducen tecnología en cuanto a transmitir datos se refiere. Este prototipo E-vote puede implementarse inicialmente el ciudades capitales cumpliendo la función básica de intercambiar datos entre el aplicativo y el servidor de manera fiable y segura utilizando los protocolos ssl/tls en entornos intranet y el protocolo ipsec hacia la extranet, con ello se minimiza de los ataques más comunes a estos sistemas, y además se cierra la brecha actual de conteo manual y transmisiones voz a voz del sistema actual.

Por ello ipsec como estándar de seguridad potente y flexible bajo diversas configuraciones punto a punto establece una comunicación segura entre dispositivos intermedios y no de extremo a extremo, por ello la solución general es complementarse con ssl/tls para establecer conexiones seguras a nivel de usuario.

Para concluir el voto electrónico en Colombia si se implementa basado en este prototipo será el primer sistema en Latinoamérica en integrar seguridad desde el mismo momento en que nace el voto en el puesto de votación como un todo; integrando autenticación y verificación del elector, encriptamiento y transmisión de los datos siendo seguro o incluso más seguro que el voto tradicional en papel si se implementan medidas de seguridad adicionales para su transporte. Protocolos como ssl/tls complementados con ipsec pueden ser utilizados en la transmisión pero no suficientes para garantizar los requisitos de seguridad específicos del voto electrónico en nuestro país. En este trabajo hemos presentado una herramienta que integra características de seguridad fundamentales a la hora de transmitir datos en procesos electorales bajo sistemas electrónicos; no obstante el voto electrónico no soluciona problemas tradicionales como trashumancia, compra y venta de votos entre otros delitos electorales muy comunes en Colombia y latinoamérica, este prototipo solo garantiza altos niveles de seguridad al sistema de votación en las fases de votación, conteo y posterior transmisión de los datos durante la jornada electoral hacia los grandes centros de datos dentro de una intranet o extranet todo en un solo sistema integrado de votación.

Dentro de las limitaciones de esta investigación solo se pudieron hacer análisis de tráfico con los ataques más comunes a estos sistemas pero ha futuro se deberá ampliar el rango de ataques para mayor credibilidad en la implementación de estos sistemas y mejorar su seguridad; además revisar nuevos protocolos seguros que garanticen la autenticación de dispositivos finales hacia los grandes data centers usando el protocolo HSTS que ya es estándar de conectividad seguro.

REFERENCIAS

[16] Aguilar, G., Sánchez, G., Toscano, K., Nakano, M., & Pérez, H. (2013). Reconocimiento de Huellas Dactilares Usando Características Locales. Revista Facultad de Ingeniería, (46), 101-109.

[9] D. Harkins and D. carrel: The Internet Key Exchange. RFC 2409.

[6] E. Rescorla. SSL and TLS, Designing and Building Secure Systems. Addison-Wesley. 2000

[7] Espinosa G Rafael. Sistemas VLSI. Guillermo Morales-Luna (2006). Una arquitectura de seguridad para IP Sección de Computación México, D.F.

[22] Espinosa Vélez María Paula, Hidalgo Betancourt Ruth Yolanda. SSL vs IPSEC. Universidad técnica particular de Loja

[6] Espinosa Vélez María Paula, Hidalgo Betancourt Ruth Yolanda. SSL, Secure Sockets Layer y Otros Protocolos Seguros para el Comercio Electrónico. Universidad Politécnica de Madrid.

[20] Fandiño Casas, L. J. (2013). Análisis de los alcances y limitaciones de la implementación del voto electrónico en América Latina, lecciones para Colombia. Doctoral dissertation, Universidad del Rosario.

[8] Francisconi, H. A. (2005). IPsec en Ambientes IPv4 e IPv6. *Versión 1.0) ISBN*, 987-43.

[5] Gálvez Muñoz, L. A. (2009). Aproximación al voto electrónico presencial: estado de la cuestión y recomendaciones para su implantación. Teoría y realidad constitucional, (23), 257-270.

[18] Maiwald, E., & Miguel, E. A. (2005). Fundamentos de seguridad de redes. McGraw-Hill.

[15] Mamani Quispe, C. (2012). Protocolos de Comunicación Utilizados en Cloud Computing. Revista de Información, Tecnología y Sociedad, 91.

[1] Min TIC, Registraduria nacional del estado civil, acta no. 020 – 2013. Comisión asesora para la incorporación, implantación y/o diseño de tecnologías de la información y las comunicaciones para el proceso electoral.

[3] Morales R Víctor M**;** (2009). Tesis doctoral; seguridad en los procesos de voto electrónico: registro, votación, consolidación de resultados y auditoria. Universidad de politécnica de Cataluña.

[17] Moya, J. M. H. (2004). RFID. Etiquetas Inteligentes. *Bit*, (146), 54-56.

[21] Onpe. Perú 2005 – 2012. Historia del voto electrónico en América Latina. Documento de trabajo 31.

[11] Pérez Iglesias Santiago (2008). Análisis del protocolo IPsec: el estándar de seguridad en IP Telefónica Investigación y Desarrollo.

[14] Padilla, j. l. v., gastelú, m. e. r., & serna, l. a. m. (2014). Un modelo de seguridad en internet utilizando sistemas distribuidos. Libro científico: investigaciones en tecnologías de información informática y Computación, 17.

[12] S. Kent and R. Atkinson: Security Architecture for the Internet Protocol. RFC 2401.

[10] S. Kent and R. Atkinson: IP Authentication Header. RFC 2402.

[8] S. Kent and R. Atkinson: IP Encapsulating Security Payload (ESP). RFC 2406.

[4] Sulbaran, Y. (2005). Evaluación de los dispositivos a nivel de la capa 2, 3 y 4 del modelo OSI. Télématique, 4(1), 87-123.

[13] Stallings, W. (2003). Fundamentos de seguridad en redes: aplicaciones y estándares. Pearson Educación.

[19] Zhe Chen, Shize Guo, Kangfeng Zheng and Yixian Yang, (2007) Modeling of Man-in-the-Middle Attack in the Wireless Networks, Wicom'07, Proceedings-Vol.1, pp.2255-2258, IEEE, Sep

[2] Zuleta, C. L. F., "Implicaciones de la adopción del voto electrónico en Colombia". Departamento Nacional de Planeación.

Raúl Bareño Gutiérrez Ingeniero de sistemas, Magister en telecomunicaciones, Dr. (c) en ciencias computacionales enfocado a la educación con TIC, UNINI México. Docente investigador de la Corporación Universitaria Minuto de Dios, (Uniminuto) grupo de investigación IT-línea de investigación de informática y tecnología. Con certificaciones internacionales en CCNA, CCNP, y FWL de cisco.

Omar Lengerke Ingeniero de Sistemas en la Universidad Autónoma de Bucaramanga UNAB- Colombia (1999), Magister en Ciencias en Control y Automatización de Sistemas de Manufactura en el Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Estado de México ITESM/CEM (2002) y Doctor en Ciencias en Ingeniería Mecánica de la Universidade Federal do Rio de Janeiro – COPPE/UFRJ, Brasil (2010).