



*V Congreso Iberoamericano
de Seguridad Informática*



Cross-Layer Security

Josep Lluís Ferrer Gomila
Antonio Urbano Fullana

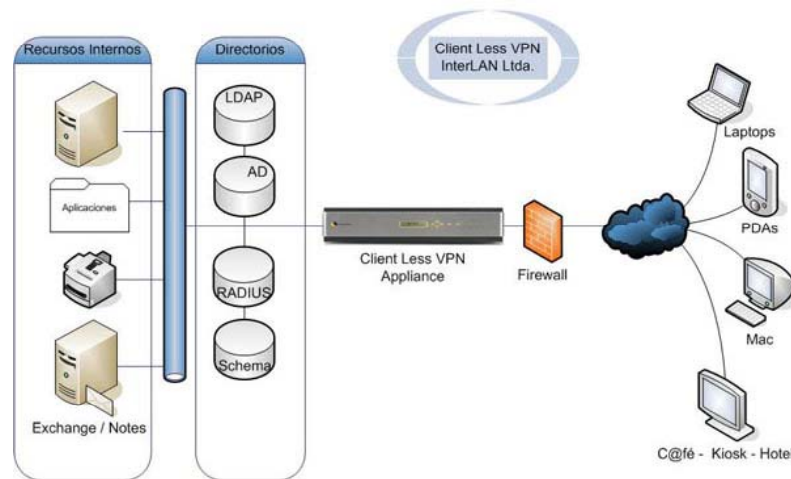


**Universitat de les
Illes Balears**



Escenarios de trabajo

- Acceso desde terminal inalámbrico (portátil, PDA, etc) a correo a través de servicio Web.
- Acceso desde terminal inalámbrico (portátil, PDA, etc) a operaciones bancarias ofrecidas por entidad.
- Acceso desde terminal inalámbrico (portátil) a bases de datos y aplicaciones de una empresa privada.





Arquitectura de Seguridad en TCP/IP.

CAPA	PROTOCOLO	MECANISMO SEGURIDAD	QUÉ NIVEL DE SEGURIDAD
APLICACIÓN	HTTP		
TRANSPORTE	TCP	SSL	CIFRADO - INTEGRIDAD
RED	IP	IPSEC	CIFRADO – INTEGRIDAD
ENLACE	802.11	WEP, TKIP, AES	CIFRADO - INTEGRIDAD
FISICA	802.11		

Se aplica cifrado en diferentes capas sobre los mismos bits de información.



Formato de trama 802.11 cifrado WEP.

	802.11	BYTES
CIFRADO 802.11 WEP RC4	802.11 HEADER	30
	LLC HEADER	8
	NEW IP HEADER	20
	ESP HEADER	16
CIFRADO IPSEC 3DES	IP HEADER	20
	TCP HEADER	20
CIFRADO SSL RC4	DATA	1460
	ESP TRAILER	4
	ESP AUTHENT	12
	FCS	4

-¿Es posible suprimir el cifrado en alguna capa?

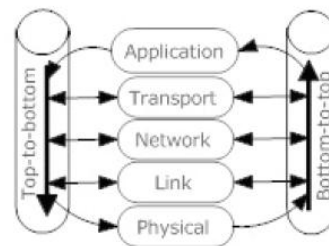
- Las capas deben disponer de información de los mecanismos de cifrado aplicados en el resto de capas.

- Se deben mantener las propiedades de seguridad individuales de capa.

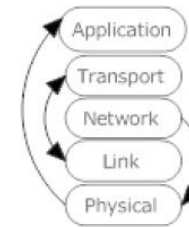


Cross-Layer

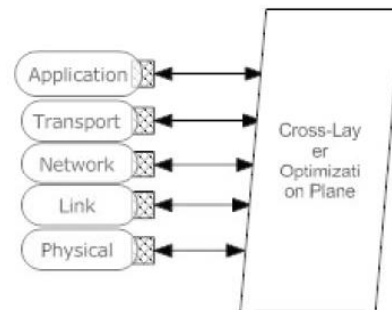
¿Son óptimos los protocolos y mecanismos tradicionales al operar en entornos inalámbricos?



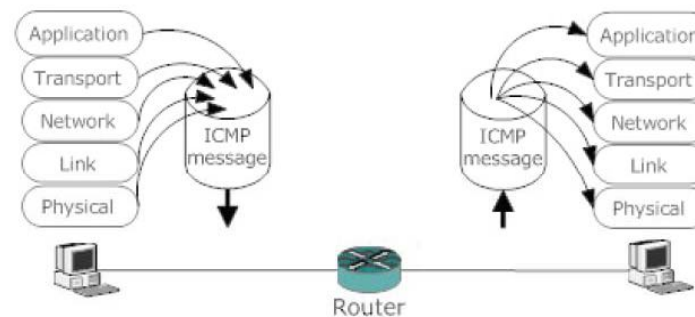
a) Interlayer Signaling Pipe



b) Direct Interlayer Communication



c) Central Cross-Layer Plane



d) Network-wide Cross-layer Signaling



Propuesta y fase de la investigación

- ¿Cuál es nuestra propuesta?
 - Apliquemos el diseño Cross-Layer para reducir las operaciones de cifrado en la arquitectura TCP/IP.
- ¿Qué ganamos?
 - Ahorro energía en terminales y optimización del ancho de banda por usuario en puntos de acceso en arquitecturas en modo infraestructura.
- Situación actual
 - Cuantificación teórica del ahorro en bytes cifrados / operaciones de cifrado.
 - Cuantificación teórica y empírica del ahorro de energía y ancho de banda en los puntos de acceso.



*V Congreso Iberoamericano
de Seguridad Informática*

2009

Gracias



**Universitat de les
Illes Balears**