LAS LEYES DE LA MECÁNICA CUÁNTICA INSPIRAN UN MÉTODO PARA ENVIAR MENSAJES CONFIDENCIALES POR INTERNET

http://www.conicet.gov.ar/las-leyes-de-la-mecanica-cuantica-inspiran-un-metodo-para-enviar-mensajes-confidenciales-por-internet/

DESCRIPCIÓN

Se trata de una tecnología que aparentemente permite transformar mensajes de correo en paquetes de lectura única empleando un sistema cliente servidor en el cual los clientes emisores redactan (y tal vez adjuntan archivos) sus mensajes en forma convencional en una página web de servidor asegurado, creando al mismo tiempo un link de descarga. El servidor se encarga de transformarlos en paquetes cuánticamente asegurados de única lectura y autodestrucción y cuando el destinatario activa el link de descarga, sólo queda en la pantalla del receptor porque se autodestruye en el servidor.

ASPECTOS POSITIVOS

Es una tecnología absolutamente original y que potencialmente puede ser perfeccionada para su empleo. No cabe duda que los mecanismos cuánticos aplicados al uso criptográfico representan parte del horizonte futuro de la seguridad informática.

ASPECTOS DESCONOCIDOS

No se conocen los detalles y potenciales vulnerabilidades de la tecnología. Queda claro que la sofisticación del servidor puede implicar costos tecnológicos que superen los recursos disponibles para su difusión masiva. Hoy día el costo comercial de un nodo cuántico para intercambio de claves oscila en los U$S 100.000. No sabemos cuál es el costo de desarrollo de este servidor y tampoco si para desarrollarlo dependemos de tecnología proveniente del exterior o si pudiésemos ser autosuficientes.

ASPECTOS NEGATIVOS

- La conexión hacia el servidor no es segura, sólo la conexión desde el servidor lo es.
- Se requiere que el servidor seguro se encuentre dentro del ámbito del Organismo que lo administra y que los corresponsales de envío y descarga estén registrados o enrolados en el mismo.
- El servidor y sus enlaces deben estar físicamente ubicados en un mismo predio, sin enlaces externos a su red interna.
- El sistema es centralizado y dependiente de un único hardware, lo que implica que se llega a una potencial denegación de servicio por sobrecarga de tráfico. Aparentemente el servidor no podría ser clonado, basándose en las propias leyes de la mecánica cuántica.

- Mientras no se conozcan todos los detalles técnicos, el protocolo representa seguridad por oscuridad y por ende vulnerable. Hay que auditarlo técnicamente para demostrar su invulnerabilidad, El uso de la mecánica cuántica no garantiza per se que no tenga flancos débiles.
- El costo de implementación podría ser limitante.