PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5337 di Venerdì 24 febbraio 2023

Siamo pronti ad affrontare il futuro prossimo della sicurezza?

A febbraio 2023 si è tenuto presso ERSI, un convegno sulla crittografia quantistica. Le informazioni offerte sono oltremodo preoccupanti ed impongono una rapida attivazione di contromisure, da parte degli specialisti di sicurezza informatica.

ERSI-European Telecommunication Standard Institute-è un ente, supportato da significativi finanziamenti dell'unione europea e di altre nazioni partecipanti, che svolge una intensa attività di produzione normativa nel settore delle telecomunicazioni. L'ente inoltre organizza periodici incontri di aggiornamento per i tecnici del settore, illustrando lo stato dell'arte in tema di sicurezza informatica. Chi scrive ha partecipato all'incontro che si è tenuto a metà di febbraio, dove relatori di altissimo livello hanno presentato lo scenario di protezione delle comunicazioni per il futuro prossimo venturo.

Ricordo ai lettori che i computer quantistici sono in grado di effettuare elaborazioni informatiche ad una velocità inconcepibile, per i computer tradizionali; è questo il motivo per cui possono essere utilizzati per effettuare tentativi di violazione degli algoritmi criptografici, che vengono correntemente utilizzati per proteggere comunicazioni critiche, sia nel settore industriale, sia nel settore della difesa, sia nel settore delle istituzioni finanziarie.

Gli esperti hanno esaminato in particolare la possibile tempistica di violazione degli algoritmi attualmente più diffusi:

- triplo DES,
- RSA (Rivest Shamir Aldeman),
- AES (Advanced Encryption system).

Oggi questi algoritmi sono ritenuti tra i più sicuri disponibili, ma una indagine, sviluppata presso i maggiori esperti del settore, ha confermato che nel giro di una decina di anni le probabilità che questi algoritmi possano essere violati dai computer quantistici superano il 60%.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

A fronte di queste considerazioni, è evidente che gli esperti di sicurezza informatica, ed in particolare gli esperti di protezione delle comunicazioni digitali, devono fin da esso attivarsi per cercare di mettere sotto controllo gli scenari futuri.

Al proposito, ricordo ai lettori che già oggi, esistono dei sistemi di distribuzione di chiavi criptografiche, che si appoggiano a sistemi chiamati QKD - quantum key distribution.

La sicurezza di questi protocolli è basata sulla pratica impossibilità di clonare o misurare gli stati quantistici che vengono trasmessi. La sicurezza dei protocolli si basa quindi non su sofisticatissimi algoritmi, ma su sofisticate tecniche di trasmissione dei dati. Oggi sono in corso di sviluppo, in varie parti del mondo delle reti QKD e vi è una urgente necessità di sviluppare delle normative specifiche, per consentire la compatibilità delle varie procedure sviluppate. Ecco perché ETSI sta operando attivamente nello sviluppare interfacce comuni e normative applicabili all'industria delle comunicazioni quantistiche.

Nel frattempo, un altro gruppo di esperti-SAGE-security algorithms group of Expert - sta sviluppando delle normative afferenti ad algoritmi criptografici ed a protocolli che possono aiutare a prevenire le frodi, accessi non autorizzati a reti pubbliche e private e cattura di dati personali. Ad oggi, gli algoritmi già sviluppati vengono correntemente utilizzate in vari contesti, come ad esempio

- 3GPP (3rd Generation Partnership Project),
- DECT (Digital Enhanced Cordless Telecommunication),
- GSM (Groupe Spécial Mobile),
- TETRA (TErrestrial Trunked Radio),
- GPRS (General Packet Radio Service).

In particolare, l'algoritmo 3GPP viene utilizzato per proteggere le reti pubbliche telefoniche, in particolare operanti nelle frequenze 5G.

Il messaggio che è stato lanciato dagli esperti, che hanno partecipato a questo convegno, è oltremodo chiaro: la crescente disponibilità di computer quantistici (ad oggi sono due i prodotti disponibili) permetterà, da un lato, di sviluppare in modo esponenziale le capacità di calcolo, ma dall'altro lato permetterà di mettere a punto tecniche di violazione degli attuali algoritmi criptografici, che dovranno essere tempestivamente aggiornati.

Adalberto Biasiotti

Licenza Creative Commons

---

www.puntosicuro.it