Intervista ad Andrea Pasquinucci sulla crittografia quantistica

Inserito da Redazione il Ven, 2005-11-04 13:36 Crittografia | IT Colloquia | Novembre 2005 | Security

IsacaRoma: Ciao Andrea e grazie per la collaborazione. Sei l'autore del quaderno CLUSIT "Aspetti di Crittografia Moderna, da DES alla Crittografia Quantistica" (pdf 860 K); vuoi presentarti e presentarci CLUSIT?

Andrea Pasquinucci: Sono un libero professionista , o se preferite un consulente freelance, mi occupo di sicurezza informatica prevalentemente a livello tecnico, sicurezza delle reti/internet, dei sistemi operativi, crittografia eccetera. Mi occupo anche di didattica, divulgazione e ricerca sempre in sicurezza informatica.

Sono membro del Comitato Direttivo e del Comitato Tecnico/Scientifico di CLUSIT, Associazione Italiana per la Sicurezza Informatica. Il principale scopo di CLUSIT è quello di favorire la diffusione a qualunque livello della consapevolezza, informazione e formazione sulla sicurezza informatica. Soci CLUSIT sono aziende, enti pubblici e privati ma anche singole persone, professionisti del settore e semplici utilizzatori di strumenti informatici che vogliono sapere di più o tenersi aggiornati in sicurezza informatica.

I Quaderni CLUSIT sono nati come una occasione in più per fornire degli approfondimenti su vari temi in sicurezza informatica. Sono concepiti come delle brevi monografie tematiche che dovrebbero essere accessibili a chiunque si interessi di sicurezza informatica.

IR: Abbiamo pubblicato altri interventi sulla crittografia, sia di docenti universitari che di divulgatori. La tua è una terza "visione": quella del consulente aziendale. Ci sono differenze con le altre due? Che tipo di reazione hai dal mercato alla tua "evangelizzazione crittografica"?

AP: Premetto che sono un consulente un po' atipico provenendo dalla carriera universitaria, ma non vedo grandi differenze rispetto agli altri punti di vista se non che, a livello aziendale, le conoscenze e persino la consapevolezza di cosa sia la crittografia oggi nelle applicazioni informatiche è veramente troppo limitata. Mi capita spesso di sentire affermazioni del tipo "il mio sistema informatico è sicuro perché i dati sono cifrati" come se la crittografia fosse la bacchetta magica che rende qualunque cosa sicura, oppure di incontrare tecnici che utilizzano applicazioni crittografiche che non hanno ben afferrato la differenza fra algoritmi simmetrici (quale 3DES) e quelli asimmetrici (quale RSA) e le loro diverse proprietà e modi di utilizzo. Spesso c'è poco interesse a "capire" e solo interesse a farsi dire quale bottone cliccare per configurare l'applicazione, il che non da molta soddisfazione professionale.

D'altra parte, quando invece insegno crittografia, sia a livello divulgativo che in corsi di formazione, aggiornamento o universitari, trovo molto interesse e partecipazione.

IR: Parliamo di crittografia quantistica. Come ti sei specializzato in questa area? Qual è la situazione ad oggi dal punto di vista delle applicazioni pratiche?

AP: "Crittografia Quantistica" è in realtà un soprannome, il nome corretto è "Quantum Key Distribution" (QKD) ovvero un sistema per creare e distribuire chiavi segrete usando particelle elementari. Detto ciò, ho incominciato ad interessarmi alla crittografia quantistica nel 1998 per un motivo molto semplice. Mia moglie, che fa ricerca in fisica teorica in università, lavora nel campo della teoria dell'Informazione Quantistica (Quantum Information) e in quegli anni incominciò ad occuparsi di crittografia quantistica quando era all'università di Ginevra. L'interesse di mia moglie è quello di un fisico teorico (ed alcuni protocolli teorici portano il suo nome) mentre il mio interesse è quello dell'informatico che conosce la fisica e la crittografia classica e cerca di capire come la crittografia quantistica può integrarsi nei protocolli crittografici odierni. Recentemente mettendo insieme i nostri diversi punti di vista, abbiamo scritto l'unico articolo scientifico che abbiamo in comune proprio sulla crittografia quantistica.

Devo anche aggiungere che all'inizio ero abbastanza scettico sulle possibilità commerciali della crittografia quantistica (e mia moglie me lo rimprovera ancora) mentre oggi vi sono già due modelli sul mercato, alcune implementazioni note, molto interesse negli ambienti militari e grossi finanziamenti e progetti da parte di EU, USA eccetera.

IR: Il Quaderno approfondisce il tema della crittografia quantistica; vuoi tentare una sintesi? Viceversa cosa consiglieresti a chi volesse approfondire l'argomento?

AP: Nella terza parte del Quaderno, dopo aver trattato nelle prime due parti della crittografia classica odierna, mi avventuro a parlare di elaboratori quantistici e crittografia quantistica. Il messaggio principale che voglio dare è che le leggi che governano le particelle elementari sono molto diverse da quelle della fisica classica che sperimentiamo ogni giorno con i nostri 5 sensi. Se da una parte questo rende difficile manipolare le particelle elementari, dall'altra parte permette di fare cose impossibili con oggetti macroscopici. In altre parole, le particelle elementari seguono la "logica quantistica" che le fa comportare in maniera molto bizzarra, permettendo agli elaboratori quantistici di fare conti altrimenti non possibili ed alla crittografia quantistica di rendere sicuro lo scambio di chiavi segrete usando particelle elementari.

Purtroppo non vi è molto materiale disponibile per approfondire questi argomenti. Vi è ovviamente una grande letteratura scientifica, qualche introduzione per informatici agli elaboratori quantistici ma ben poco a livello divulgativo od intermedio sulla crittografia quantistica.

Per questo oltre al Quaderno CLUSIT, anch'io ho scritto qualche documento che si può trovare sul mio sito.

IR: Chi sono i "guru" della crittografia quantistica a livello mondiale? In Italia c'è qualche caso di eccellenza?

AP: Per quanto riguarda la ricerca universitaria va senza dubbio citato il gruppo di Ginevra che è forse il gruppo che ha prodotto il maggior numero di risultati sia teorici che sperimentali; vi sono poi i gruppi di Vienna (Austria) , Erlangen e Monaco (Germania), Cambridge (Regno Unito), Boston e Caltech (USA), Waterloo (Canada), Singapore ed ovviamente molti altri.

In Italia c'è il gruppo di Pavia più qualche ricercatore indipendente.

In Italia posso citare anche altri gruppi, quale uno presso il Politecnico di Milano ed uno presso l'università di Roma, che si occupano di aspetti vicini alla crittografia quantistica.

Per la parte commerciale, IdQuantique (spinoff dell'università di Ginevra) e MagiQ (New York) hanno ciascuna in vendita un modello commerciale ormai stabile. Altre aziende, quali Toshiba e NEC , hanno progetti di sviluppo che potrebbero anche presto portare nuovi modelli sul mercato. Per l'Italia posso citare ELSAG (gruppo Finmeccanica) a Genova che ha un progetto di R&S in crittografia quantistica.

IR: All'ultimo SMAU sei stato relatore del seminario sulla crittografia quantistica. Come è andata l'esperienza?

AP: Non era la prima volta che avevo l'opportunità di fare un po' di divulgazione su questi argomenti. A SMAU, come negli altri casi, ho trovato una buona partecipazione, sempre superiore alle mie attese, grande interesse e tante domande. Questo mi fa molto piacere perché, indipendentemente dal successo commerciale o meno della crittografia quantistica, ritengo che queste siano tematiche e tecnologie che faranno parte del nostro futuro.

IR: Grazie Andrea e buon lavoro

AP: grazie a voi

Chi è Andrea Pasquinucci?

Andrea Pasquinucci, PhD in fisica teorico-matematica, per 10 anni ha fatto ricerca universitaria ed insegnamento presso laboratori di ricerca ed università per lo più all'estero. Dal 2000 è un libero professionista in sicurezza informatica. Si occupa anche di insegnamento, formazione, divulgazione e ricerca in alcuni aspetti di sicurezza informatica.

E' membro del Comitato Direttivo e del Comitato Tecnico-Scientifico CLUSIT (Associazione Italiana per la Sicurezza Informatica), è socio fondatore e membro del Comitato Direttivo di AIPSI (Associazione Italiana di Professionisti della Sicurezza Informatica, capitolo Italiano di ISSA), è socio AIEA (Associazione Italiana Information Systems Auditors, capitolo di Milano di ISACA) ed è certificato CISA

Contatti: http://www.ucci.it/it/index.html