Network security: confidentiality in WPA-personal

Enrico Rizzardi 75789

Informatica specialistica curriculum sistemi e impianti

Il progetto da me sviluppato ha lo scopo di violare la confidenzialità di reti WiFi basate su WPA2-PSK, assumendo la conoscenza della chiave PSK.

Il programma da me sviluppato permette di decifrare il traffico WPA2-PSK sia in modalità live che da stream salvato su file. Esso è inoltre in grado di decifrare il traffico di più terminali mobili collegati al medesimo access-point.

Il sistema si articola in due moduli principali: uno dedicato all'analisi del traffico e alla derivazione delle chiavi effimere e l'altro alla decifratura e visualizzazione dell'output.

Il primo modulo è scritto in linguaggio C. Per effettuare lo sniffing del traffico e la decapsulazione dei dati sfrutta le librerie pcap, per il calcolo delle chiavi effimere utilizza invece le librie OpenSSL.

Il secondo modulo è scritto in Python e si appoggia alle librerie Cryptopy per decifrare i dati cifrati con AES.

Per quanto riguarda la comunicazione tra i due processi viene utilizzato un meccanismo di internet socket, il modulo sniffer implementa il client e l'altro modulo implementa il server.