Tác hại khi dùng cain & abel

Có thể được dùng cho các mục đích xấu: lấy password, nghe lén, giải mã password….

Có thể mất ndữ liệu trong quá trình sử dụng

**Nguyen ly hoat dong**

**Brute-Force attack:**

là phương pháp phá vỡ thuật toán mã hóa bằng cách thử mỗi từ khóa. Tính khả thi phụ thuộc vào độ dài của mật khẩu

Số lượng từ khóa dùng để dò được tính bằng công thức

KS = L^(m) + L^(m+1) + L^(m+2) + ........ + L^(M)

Trong đó

L = character set length

m = min length of the key

M = max length of the key

Ví dụ khi bạn muốn tìm 1 mật khẩu với các ký tự sau "ABCDEFGHIJKLMNOPQRSTUVWXYZ" tất cả là 26 ký tự, brute-force cracker sẽ dò tìm với KS = 26^1 + 26^2 + 26^3 + ...... + 26^7 = 8 353 082 582 từ khóa. Tương tự với "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&\*()-\_+=~`[]{}|\:;"'<>,.?/", the number of keys to try rises at 6 823 331 935 124.

**Dictionary attack**

là phương pháp tấn công dùng những từ khóa có sẵn trong một list cho trước.

Trong từ điển có thể có từ “password “. Kiểu tấn công này tự động dò tìm và phụ thêm các ký tự đảo ví dụ như “drowssap” hoặc tự động thêm các con số ví dụ như password00, password99.. hoặc là tự viết hoa các ký tự ví dụ Password, pAssword ,… , password.

**Nghe lén VoIP**

Sniffer chiết xuất các thông số phiên RTP như cổng RTP, người gọi / địa chỉ IP và trả lời các kiểu codec động từ SIP hoặc MGCP phiên trước các luồng dữ liệu trên RTP. Sau đó nó bắt và giải mã âm thanh RTP mã hóa với các codec sau: G711 ulaw, G771 alaw, ADPCM, DVI4, LPC, GSM610, Microsoft GSM, L16, G729, Speex, iLBC, G722.1, G723.1, G726-16 , G726-24, G726-32, G726-40, LPC-10, SIREN, LRWB-16kHz. Sau khi giải mã âm thanh được lưu vào mono hoặc WAV âm thanh stereo trên đĩa cứng của bạn