

# Le password sicure vi rendono più sicuri

Di Bruce Schneier

Traduzione di Sergio Meinardi – [smeinardi@acm.org](mailto:smeinardi@acm.org) – L'autore originale mantiene i diritti sull'opera

Chi vuole usare questo documento deve chiedere il permesso a Bruce Schneier

## Chi è Bruce Schneier?



Bruce Schneier è un autore e un rinomato esperto di sicurezza a livello internazionale. Descritto dal *The Economist* come un “guru della sicurezza”, è meglio noto come un lucido commentatore e sincero critico di tutto ciò che riguarda la sicurezza. Quando qualcuno vuole sapere come funziona veramente la sicurezza, si rivolge a Schneier.

Il suo primo bestseller, *Applied Cryptography*, spiegava come funziona la scienza arcaica dei codici segreti, e fu descritto da *Wired* come “il libro che la NSA non voleva fosse mai pubblicato”. Il suo libro sulla sicurezza di computer e reti *Secret and Lies* fu definito da *Fortune* “un scatola piena di preziose sorprese che potete usare”. *Beyond Fear* parla dei problemi della sicurezza, dai più piccoli ai più grandi: sicurezza personale, crimine, sicurezza aziendale, sicurezza nazionale. Il suo ultimo libro, “Schneier on Security”, offre delle intuizioni dal rischio del furto di identità (grandemente sopravvalutato) al pericolo di un potere presidenziale incontrollato fino al sorprendentemente semplice modo di falsare le elezioni a prova di brogli

Regolarmente citato sui media, ha testimoniato circa la sicurezza davanti al Congresso degli Stati Uniti in diverse occasioni e ha scritto articoli per le maggiori testate, quali *The New York Times*, *The Guardian*, *Forbes*, *Wired*, *Nature*, *The Bulletin of the Atomic Scientists*, *The Sydney Morning Herald*, *The Boston Globe*, *The San Francisco Chronicle*, and *The Washington Post*

Schneier pubblica una newsletter gratuita mensile, *Crypto-Gram*, con oltre 150.000 lettori. Nei 10 anni di pubblicazione regolare, *Crypto-Gram* è diventato uno dei forum più letti per discussioni a ruota libera, critiche mirate e seri dibattiti circa la sicurezza. Come fiero ed ostico conduttore, Schneier spiega, demistifica e attinge lezioni dalle storie della sicurezza che appaiono nelle notizie quotidiane.

L'autore mantiene i diritti

## Le password sicure vi rendono più sicuri

---

Di Bruce Schneier

Wired News

15 Gennaio , 2007

Da quando ho scritto circa le 34.000 password di MySpace che ho analizzato, molte persone hanno iniziato a chiedermi come scegliere password sicure.

A parte la mia opinione, è stato scritto molto su questo argomento durante gli ultimi anni, sia seriamente che in allegria, ma per la maggior parte sembra basato sulla suggestione di aneddoti piuttosto che sull'attuale prova analitica. Ciò che segue sono suggerimenti seri.

L'attacco di cui ragiono è l'attacco offline di tipo "indovina-la-password". Questo attacco presume che l'attaccante abbia una copia del documento criptato, o un file di password criptate del server, e può tentare password più veloce che può. Esistono situazioni in cui un simile attacco non ha senso. Ad esempio, le carte bancomat sono sicure anche se hanno un PIN di 4 cifre, perché non si può operare offline per indovinare il PIN. E la polizia preferisce avere un avviso di garanzia relativo al vostro account hotmail piuttosto che scoprire la vostra password dell'email. Il vostro sistema di chiave criptata tenuta presso terzi sarà più vulnerabile della vostra stessa password, così come "la domanda segreta" che avete impostato nel caso che vi scordiate la password.

L'autore mantiene i diritti

I cacciatori di password hanno acquisito velocità e intelligenza. AccessData vende il Password Recovery Toolkit (PRTK). A seconda del software che sta attaccando, PRTK può provare centinaia di migliaia di password al secondo, e comincia dalle password più comuni piuttosto che dalle più oscure.

Quindi la sicurezza delle vostre password dipende da due cose: ogni dettaglio del software che rallenta la ricerca della password e in che ordine programmi come PRTK indovinano differenti password.

Alcuni programmi includono funzioni messe lì deliberatamente per rallentare i tentativi di indovinare la password. I buoni software di criptazione non usano la vostra password come chiave di criptazione; esiste un processo che converte la vostra password in una chiave di criptazione. E il software può eseguire questo processo lentamente quanto vuole.

I risultati sono ovunque. Microsoft Office, per esempio, ha una semplice conversione password-chiave, così PRTK può testare 350.000 password Word per secondo su un Pentium IV a 3GHz, che è un riferimento piuttosto ragionevole. WinZip era ancora peggio, ben oltre il milione di tentativi al secondo per la versione 7.0, ma con la versione 9.0 la funzione di complicazione del sistema criptografico è stata sostanzialmente migliorata: PRTK può testare solo 900 password al secondo. Anche PGP rende le cose deliberatamente complicate a programmi tipo PRTK, permettendo circa 900 tentativi al secondo.

Quando si attaccano programmi con sistemi deliberatamente rallentanti, è importante fare i conteggi dei tentativi. Un semplice attacco esaustivo su 6 caratteri minuscoli, da “aaaaaa” a “zzzzzz”, ha più di 308 milioni di combinazioni. Ed è generalmente improduttivo, perché il programma

perde la maggior parte del proprio tempo testando improbabili password come “pqzrwj”.

Secondo Eric Thompson di AccessData, una password tipica consiste di una radice più un'appendice. La radice non è necessariamente una parola di dizionario, ma è qualcosa di pronunciabile. Un'appendice può essere sia un suffisso (90% delle volte) che un prefisso (10% delle volte).

E' per questo che il primo attacco di PRTK consiste nel testare un dizionario di circa 1000 password comuni, cose come “letmein” [ricordate che l'articolo è scritto con riferimento alla lingua inglese, *ndt*], “password1”, “123456” e via dicendo. Poi si passa a testare le stesse con circa 100 suffissi comuni: “1”, “4u”, “69”, “abc”, “!” ecc. Che ci crediate o no, si trovano il 24% di tutte le password con queste 100.000 combinazioni.

Poi PRTK continua con una serie di complessità crescente di radici prese dal dizionario e appendici, anch'esse prese dal dizionario. Le radici includono:

- Comuni parole di dizionario: 5.000 voci
- Dizionario dei nomi: 10.000 voci
- Dizionario completo: 100.000 voci
- Dizionario dei modelli fonetici: 1/10.000 di una ricerca esaustiva di caratteri

Il dizionario dei modelli fonetici è interessante. Non è un vero dizionario; è una funzione matematica basata sulle code di Markov che genera insiemi di caratteri pronunciabili in inglese di una data lunghezza. Per esempio PRTK può generare e testare un dizionario di parole di 6 caratteri veramente pronunciabili, o parole di sette caratteri

appena pronunciabili. Stanno lavorando sulle funzioni di generazione per altre lingue.

PRTK esegue anche una ricerca esaustiva di parole di 4 caratteri. Usa il dizionario con parole minuscole (le più comuni), con l'iniziale maiuscola (le seconde più comuni), tutte maiuscole e la finale maiuscola. Prova anche sostituzioni comuni: “\$” per “S”, “@” per “a”, “1” per “l” e così via.

I dizionari delle appendici comprendono cose come:

- Tutte le combinazioni di due cifre
- Tutte le date dal 1900 a oggi
- Tutte le combinazioni di tre cifre
- Tutti i simboli singoli
- Tutte le singole cifre più i singoli simboli
- Tutte le combinazioni di due simboli

L'ingrediente segreto della ricetta di AccessData è l'ordine in cui le varie radici e appendici vengono combinate. Le ricerche della società indicano che la password più gettonata ha da 7 a 9 caratteri per la radice più un'appendice comune, ed è più comune che una persona scelga una radice difficile da indovinare piuttosto che un'appendice non comune.

Di solito, PRTK viene lanciato da una rete di computer. Indovinare una password è un banale compito e può essere eseguito in background. Una grande organizzazione come i Servizi Segreti possono avere facilmente centinaia di computer impegnati sulla password di qualcuno. Una società chiamata Tableau sta costruendo uno speciale hardware (FPGA) per aumentare la velocità di PRTK con programmi come PGP e Winzip: un aumento di prestazioni di 150-300 volte.

L'autore mantiene i diritti

Quanto è bene tutto questo? Eric Thompson stima che avendo a disposizione da due settimane a un mese di tempo, il suo software scopre dal 55% al 65 di tutte le password. (dipende molto, ovviamente, dall'applicazione). Buoni risultati, ma non grandi.

Ma qui non abbiamo considerato i dati biografici. Quando è possibile, AccessData colleziona tutti i dati personali possibili sul soggetto titolare della password, prima di cominciare. Se può vedere altre password, può fare supposizioni sul tipo di password usate dal soggetto. Quanto è lunga la parola radice? Che genere di radice? Mette l'appendice dopo o prima della radice? Usa le sostituzioni? I codici CAP sono appendici comuni, quindi vengono immessi nel processo. Come pure indirizzi, nomi dall'agenda, altre password e ogni altra informazione personale. Questi dati aumentano il successo di PRTK, ma, più importante, riducono il tempo necessario da settimane a giorni o addirittura ore.

Quindi, se volete che la vostra password sia difficile da indovinare, dovete scegliere qualcosa che non sia nelle liste delle radici e delle appendici. Dovete mischiare minuscole e maiuscole nel mezzo della vostra radice. Dovreste aggiungere numeri e simboli nel mezzo della vostra radice, ma non comuni sostituzioni. O mettete l'appendice nel mezzo della radice. O usate due radici con in mezzo un'appendice.

Persino qualcosa di più semplice presente nella lista del dizionario PRTK, il dizionario dei modelli fonetici, insieme a un'appendice non comune, può essere difficile da indovinare. Come pure una password fatta con le iniziali delle parole di una frase, specialmente se ci mettete anche numeri e simboli. E sì, queste password possono essere difficili da ricordare, che è il motivo per cui dovrete usare un programma gratuito e open source come Password Safe per memorizzarle tutte. (PRTK può testare solo 900 password al secondo contro Password Safe).

L'autore mantiene i diritti

Anche così, niente di questo potrebbe essere interessante. AccessData vende un altro programma, Forensic Toolkit, che, tra le altre cose, cerca su un hard disk ogni insieme di caratteri stampabili. Cerca nei documenti, nel Registry, nelle email, nei file di swap, nei file cancellati, ovunque. E crea un dizionario da questo e lo dà in pasto a PRTK. E PRTK scova più del 50% delle password con questo solo dizionario.

Quel che succede è che la gestione della memoria di Windows lascia dati ovunque durante il normale lavoro. Voi digitate una password e viene messa memorizzata da qualche parte. Windows la scrive su un file temporaneo. Viene messa in un posto recondito dell'hard disk e lì rimane per sempre. Linux e MacOS non sono meglio.

Voglio far notare che niente di questo ha a che fare con algoritmi di cifratura o lunghezza della chiave. Un algoritmo debole a 40 bit non rende l'attacco più semplice, e un algoritmo forte a 256 bit non lo rende più difficile. Questi attacchi simulano il processo di inserimento della password, quindi la dimensione della chiave non è un problema.

Per anni ho detto che il modo più semplice per rompere un prodotto crittografico non consiste quasi mai nel decifrare l'algoritmo, ma che quasi invariabilmente c'è un errore di programma che permette di bypassare i fondamenti matematici e rompere il prodotto. Una cosa simile succede qui. Il modo più semplice di indovinare una password non è indovinarla, ma sfruttare le insicurezze del sistema operativo sottostante.

Quanto sono buone le password che la gente sceglie per proteggere il proprio computer e gli account online?

E' una domanda difficile a cui rispondere perché i dati sono scarsi. Ma recentemente, un collega mi ha mandato alcuni dati presi da MySpace durante un attacco di phishing: 34.000 nomi utente e password.

L'attacco fu piuttosto semplice. Gli assalitori hanno creato una finta pagina di login di MySpace e hanno collezionato le informazioni di login quando gli utenti pensavano di accedere al proprio account. I dati erano inoltrati a vari server compromessi, da dove gli attaccanti li avrebbero raccolti più tardi.

MySpace stima che più di 100.000 persone sono cadute nel tranello prima che l'attacco venisse terminato. I dati in mio possesso arrivano da due differenti punti, e sono stati puliti dalla piccola percentuale di persone che avevano capito di essere sotto attacco phishing. Ho analizzato i dati e questo è ciò che ho imparato.

**Lunghezza della password:** Mentre il 65% delle password contengono 8 caratteri o meno, il 17% sono di 6 caratteri o meno. La password media è lunga 8 caratteri.

In particolare, la distribuzione delle lunghezze è la seguente:

1-4	0.82 %
5	1.1 %
6	15 %
7	23 %
8	25 %
9	17 %
10	13 %
11	2.7 %
12	0.93 %
13-32	0.93 %

Sì, c'era una password di 32 caratteri: "1ancheste23nite41ancheste23nite4." Altre password lunghe erano "fool2thinkfool2thinkol2think" e "dokitty17darling7g7darling7."

**Mix di caratteri:** mentre l'81% delle password sono alfanumeriche, il 28% sono solo lettere minuscole più una cifra finale – e due terzi di queste hanno la singola cifra 1. Solo il 3.8% delle password sono singole parole di dizionario, e un altro 12% sono una singola parola di dizionario più una cifra finale – ancora una volta, due terzi delle volte la cifra è 1.

Solo numeri	1.3 %
Solo lettere	9.6 %
Alfanumeriche	81 %
Non alfanumeriche	8.3 %

Solo lo 0.34% degli utenti hanno la porzione di nome utente del proprio account email come password.

**Password comuni:** Le prime 20 password sono (in ordine)

*password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 and monkey.*

La password più comune, "password1", è stata usata nello 0.22% dei casi. La frequenza diminuisce velocemente: "abc123" e "myspace1" sono stati usati solo nello 0.11% dei casi, "soccer" nello 0.04% e "monkey" nello 0.02%. (Ricordiamoci che stiamo parlando di utenti di lingua inglese, ndt)

Per chi non lo sa, Blink 182 è una band. Presumibilmente molte persone usano il nome della band perché contiene numeri nel nome e, perciò, sembra una buona password. La band SlipKnot non ha numeri nel nome, il che spiega la presenza dell'1. La password "jordan23" fa

riferimento al giocatore dei basket Michael Jordan e al suo numero. E, naturalmente, “myspace” e “myspace1” sono facili da ricordare per un account MySpace. Non so come spiegare “monkey”.

Si diceva che “password” fosse la password più comune. Ora è “password1”. Chi ha detto che gli utenti non hanno imparato niente sulla sicurezza?

Comunque, seriamente, le password stanno migliorando. Mi impressiona che solo il 4% fossero parole di dizionario e che la maggior parte fossero alfanumeriche. Nel 1989, Daniel Klein era in grado di scoprire il 24% delle password con un dizionario di 63.000 parole e trovava che la lunghezza media fosse di 6.4 caratteri.

E nel 1992 Gene Spafford scoprì il 20% delle password con il proprio dizionario e trovò che la lunghezza media era di 6.8 caratteri (entrambi studiarono password Unix, che avevano un limite massimo di 8 caratteri). Ed entrambi riportarono una stragrande maggioranza di tutto minuscolo e qualche maiuscolo-minuscolo, rispetto a quanto emerso nei dati di MySpace. Il concetto di scegliere buone password si sta inculcando nelle persone, almeno un po’.

Peraltro, chi partecipa a MySpace è piuttosto giovane. Un altro studio fatto a novembre verificò le password di 200 impiegati di una grande società: 20% solo lettere, 78% alfanumeriche, 2.1% con caratteri non alfanumerici e lunghezza media 7.8 caratteri. Meglio di 15 anni fa, ma non buone come quelle di MySpace. I ragazzi sono veramente il futuro.

Niente cambia la realtà che queste password hanno mantenuto la propria utilità come un curioso dispositivo di sicurezza. Negli anni, i ladri di password sono diventati molto più veloci. I prodotti commerciali attuali possono testare decine – persino centinaia – di milioni di password per secondo. Allo stesso tempo, esiste una complessità massima della password che le persone sono disposte a

memorizzare. Questi limiti sono stati superati anni fa e le tipiche password del mondo reale sono ora indovinabili via software. PRTK di AccessData sarebbe stato in grado di scoprire il 23% delle password MySpace in 30 minuti, il 55% in 8 ore.

Naturalmente, questa analisi assume che l'assalitore può mettere le mani sul file criptato delle password e lavorarci su non essendo collegato, a proprio piacimento; cioè, che la stessa password fosse usata per criptare una mail, un file o un hard disk. Le password funzionano ancora se potete evitare gli attacchi offline. Sono utili anche in situazioni di sicurezza di basso valore, o se scegliete password veramente complicate e usate qualcosa come Password Safe per memorizzarle. Altrimenti, la sicurezza con la password da sola è piuttosto rischiosa.