UNA PROPOSTA PER LA CONDIVISIONE SICURA DELLE PASSWORD DI ACCESSO AI BBS PACKET RADIO.

Marco Savegnago IW3FQG
Aprile 1998

Revisione 3

Le password per accedere ai BBS Packet-Radio. Un po' di storia…

L'accesso ai BBS regolato da password fu introdotto per la prima volta dalle nostre parti nel novembre 1991 per impedire accessi ai BBS radioamatoriali da parte di stazioni non autorizzate e abusi di nominativo ad opera anche di stazioni autorizzate. All'inizio, questa nostra scelta, fu giudicata contraria all'ham-spirit e generalmente bocciata dal resto della comunità radioamatoriale. Con gli anni poi praticamente tutti i BBS attivi in Italia hanno cominciato a utilizzare la password come sistema di protezione sia per gli utenti (che cosi' evitano che il loro nominativo sia usato se non attivi in packet-radio e per garantire che non ci siano sostituzioni di persona) che per i gestori di BBS (per analoghi motivi che non e' qui il caso di discutere).

La password utilizzando l'algoritmo denominato a matrice (derivato da NETROM)

All'inizio l'autenticazione dell'identità dell'utente era effettuata solo grazie all'algoritmo derivato da NET/ROM, ribattezzato negli anni a matrice, che consiste in una richiesta casuale fatta dal BBS di 5 o più numeri alla quale l'utente deve rispondere con le lettere corrispondenti al numero richiesto nella chiave che egli ha comunicato al gestore del BBS (Sysop).

L'algoritmo funziona in questo modo:

L'utente invia al Sysop del BBS via posta una chiave alfanumerica (che può essere mnemonica) lunga al minimo 5 caratteri e una copia di documenti che ne certifichino l'identità , il Sysop una volta verificato che non ci siano problemi provvederà a inserirla nel file di configurazione del programma di controllo di accesso del BBS.

Il protocollo di autenticazione funziona in modo testo, non richiede particolari programmi e può venire eseguito anche mentalmente o con l'aiuto di carta e penna dall'utente.

All'atto della connessione il BBS genera 5 o più numeri casuali che corrispondono a 5 o più lettere della frase e le invia all'utente. Se la frase inviata al Sysop era composta dalle prime 10 lettere dell'alfabeto lo schema seguito sarà:

```
                  1
1 2 3 4 5 6 7 8 9 0

A B C D E F G H I J
```

Il prompt con la richiesta di autenticazione segue all'incirca il seguente modello:

? Password <I3KUH:N5> 1 2 3 4 5

Questa richiesta viene in gergo chiamata **challenge.**

Normalmente se la chiave contiene degli spazi, questi non sono richiesti ma sono considerati per il conteggio delle lettere.
L'utente come risposta invia le cinque lettere corrispondenti ai numeri richiesti.
(es. ABCDE)

La risposta inviata potrà essere corretta o no, in ogni caso il BBS richiederà nuovamente una password.
L'utente ha facoltà di decidere se entrare nel sistema (ammesso che abbia inviato la password corretta) inviando un semplice carattere <INVIO>, interrogare il sistema per sapere se una delle password fino a quel punto inviate era corretta (inviando il carattere '?' seguito dal carattere di invio), oppure inviare una nuova password.
Questa fase durerà finche' non sarà riuscito a formulare una risposta corretta o avrà deciso di terminare di confondere le idee a eventuali ascoltatori interessati.

Subito, vista la semplicità con cui e' possibile trovare l'intera frase utilizzata fu introdotta la possibilità di rispondere con lettere casuali facenti parte di gruppi prefissati in modo da confondere le idee a eventuali ascoltatori interessati.

Data la semplicità dell'algoritmo non mi dilungo su quali possono essere i metodi (più o meno automatici) che consento di ricostruire con il semplice monitoraggio del canale, l'intera frase.
Se a questo si applica un semplice analizzatore di frasi che 'pesca' da un dizionario di frasi prefabbricate la cosa diventa ancora più semplice.

Vantaggi e svantaggi dell'algoritmo denominato a matrice

Vantaggi:

1. Algoritmo elementare, immediato, semplice da implementare o da realizzare anche senza uso del computer
2. Esistono numerosi programmi che gestiscono in modo nativo l'algoritmo

Svantaggi:

1. Scarsa sicurezza dovuta al fatto che componenti della password vengono trasmessi in un canale insicuro
2. Scarso numero di combinazioni possibili che rendono vulnerabile il sistema già con un semplice attacco condotto 'a mano'
3. Possibilità che un Sysop disonesto o hackers si impadroniscano della chiavi e siano in grado di sostituirsi a lui completamente. Impossibile quindi usare questo protocollo per condividere la password tra BBS.

Esistono altri metodi di autenticazione simili a questo e come questo altamente insicuri vedi ad esempio quelli impiegati nella rete ITANET o FLEXNET (SuperVozelj usa la stessa di NETROM…) nei quali le apparenti complicazioni introdotte dagli autori nel calcolo delle soluzioni servono solo a limitare la possibilità di errore da parte degli hackers nel cercare la chiave corretta...

La password utilizzando l'algoritmo MD2

Alla fine del 1992 fu introdotto il metodo di autenticazione dell'utente utilizzando l'algoritmo RSA MD2.

La caratteristica dell'algoritmo MD2 e' che data una qualsiasi serie di caratteri (provenienti da uno stream di dati o da una semplice stringa) in ingresso, produce in uscita una chiave detta in gergo fingertip univoca (dato l'ingresso), unidirezionale (nel senso che non e' sufficiente per ricavare la chiave di origine di ingresso) e di lunghezza fissa. In pratica una specie di impronta digitale univoca.

Il protocollo di autenticazione dell'utente con algoritmo MD2 funziona cosi':

L'utente invia al Sysop del BBS via posta una chiave alfanumerica (che può essere mnemonica) lunga al minimo 5 caratteri e una copia di documenti che ne certifichino l'identità , il Sysop una volta verificato che non ci siano problemi provvederà a inserirla nel file di configurazione del programma di controllo di accesso del BBS.

All'atto della connessione il BBS può generare un multi **challenge** che consente all'utente di scegliere quale protocollo utilizzare per l'autenticazione, oppure un solo **challenge** se l'utente ha deciso di collegarsi utilizzando sempre e solo una protocollo. (In base al protocollo utilizzato il BBS potrebbe decidere se aumentare o diminuire il livello di sicurezza attribuito all'utente)

Il BBS invia la proposta di autenticazione formata dal prompt (con l'header indicante i protocolli supportati) e il **challenge**

? Password <I3KUH:N5-MD2> 1 2 3 4 5 [0123456789]

oppure

? Password <I3KUH:N5-MD2> [0123456789]

dove il **challenge** MD2 e' quello compreso tra parentesi quadre.
Se l'utente e' in grado di rispondere utilizzerà il protocollo più sicuro tra quelli disponibili (e indicati nell'header del prompt).
Contemporaneamente il BBS esegue la funzione MD2 usando come valore di ingresso il **challenge** MD2 e la chiave conosciuta dall'utente.
L'utente (che conosce la sua chiave) dato il **challenge** MD2 produce lo stesso risultato e lo invia al BBS.
Se il risultato calcolato dal BBS corrisponde a quello ricevuto dall'utente allora il processo di autenticazione, e' completato.

Sfruttando questa caratteristica e' possibile essere sicuri che BBS e utente si scambino il **challenge** senza che la chiave segreta passi nel canale radio insicuro.

Dal punto di vista della sicurezza l'impiego di MD2 con la chiave fissa unita al **challenge** variabile e dipendente dalla sessione consente di essere abbastanza tranquilli.
Tentare un attacco con il metodo a forza bruta dell'algoritmo non e' certamente conveniente visto l'esiguità della posta in gioco… Ma per puro scopo sperimentale sarebbe interessante misurare la sicurezza dell'impiego di chiavi non casuali visto che la maggior parte delle frasi utilizzate hanno un senso compiuto o si rifanno al nome e cognome dell'utente o dei familiari.

Vantaggi e svantaggi dell'algoritmo MD2

Vantaggi:

1. Algoritmo diffuso semplice, veloce e (nel contesto usato) sicuro
2. Nessuna componente delle chiavi viene trasmessa nel canale insicuro
3. Elevato livello di sicurezza dell'algoritmo di codifica unito all'impiego di un **challenge** pseudo casuale generato ad ogni collegamento.
4. Possibilità di usare chiavi mnemoniche

Svantaggi:

1. Possibilità che se un hacker forza un sistema possa utilizzare la chiave indisturbato per accedere a qualunque altro sistema presente in rete
2. Impossibilita' di calcolare 'a mano' il risultato
3. Possibilità che un Sysop disonesto o hackers si impadroniscano della chiavi e siano in grado di sostituirsi a lui completamente. Impossibile quindi usare questo protocollo per condividere la password tra BBS.

La password utilizzando l'algoritmo RSA a chiavi asimmetriche

Oggi grazie alla diffusione delle reti a livello regionale o nazionale, la scomodità di avere password diverse tra BBS oppure il solo fatto di dover essere registrati in ogni BBS ha fatto nascere la necessità di disporre di un sistema di autenticazione più evoluto che consenta di:

1. Utilizzare la stessa password in più BBS (sia a livello regionale che nazionale)
2. Evitare che il Sysop, eventuali sostituiti o semplicemente hackers che riescano a forzare un sistema siano poi in grado di entrare liberamente in qualunque BBS per vari scopi.

La soluzione e' quella di utilizzare un protocollo di autenticazione che faccia uso di un algoritmo di cifratura con chiavi asimmetriche

Un algoritmo a chiavi asimmetriche consente all'utente di generare una coppia di chiavi:

1. una chiave liberamente condivisibile (detta pubblica) con tutte le BBS che a lui interessa collegare e utile solo a decodificare il **challenge** all'atto della connessione
2. una chiave (detta privata) che terra' per se' e che gli consente di codificare il **challenge**.

Il protocollo di autenticazione dell'utente funziona cosi':

L'utente utilizzando un apposito programma genera la coppia di chiavi.
Invia al Sysop del BBS quella pubblica con una copia di documenti che ne certifichino l'identità, il Sysop una volta verificato che non ci siano problemi provvederà a inserirla nel file di configurazione del programma di controllo di accesso del BBS.
Una soluzione al problema di dover registrare la propria password presso qualunque BBS a cui si vuol accedere e quella di istituire a livello regionale un archivio certificato delle chiavi pubbliche che certifica l'autenticità dei dati distribuiti e provvede ad aggiornare gli archivi dei BBS collegati in rete. In questo modo un utente che si e' registrato sa' di poter entrare in tutti i BBS della rete.

All'atto della connessione il BBS può generare un multi **challenge** che consente all'utente di scegliere quale protocollo utilizzare per l'autenticazione, oppure un solo **challenge** se l'utente ha deciso di collegarsi utilizzando sempre solo un protocollo sicuro. (In base al protocollo utilizzato il BBS potrebbe decidere se aumentare o diminuire il livello di sicurezza attribuito all'utente)

Il BBS invia la proposta di autenticazione formata dal prompt (con l'header indicante i protocolli supportati) e il **challenge**

? Password <I3KUH:N5-MD2-RSA128> 1 2 3 4 5 [0123456789]

dove il **challenge** RSA e' uguale a quello MD2 e' quello compreso tra parentesi quadre per evitare problemi di compatibilità all'indietro con i programmi già esistenti.
Se l'utente e' in grado di rispondere, utilizzerà il protocollo più sicuro tra quelli disponibili (e indicati nell'header del prompt).

L'utente riceve il **challenge** RSA, esegue la funzione MD2 in modo da ottenere in ingresso una chiave di lunghezza prefissata, codifica il risultato della funzione MD2 con la sua chiave privata e invia il risultato al BBS.
Il BBS riceve il risultato, lo decodifica con la chiave pubblica dell'utente e lo compara con il risultato della funzione MD2 eseguita da lui localmente sul **challenge** MD2. Se i due risultatati combaciano allora l'utente, e' autenticato.

Vantaggi e svantaggi dell'algoritmo RSA

Vantaggi:

1. Nessuna delle chiavi viene trasmessa nel canale radio insicuro
2. Possibilità di condividere la stessa chiave pubblica tra BBS
3. Elevato livello di sicurezza dell'algoritmo di codifica unito all'impiego di un **challenge** pseudo casuale generato ad ogni collegamento.

Svantaggi:

1. Impossibilita' di usare chiavi mnemoniche
2. Impossibilita' di calcolare 'a mano' il risultato

Note:

Questa implementazione e' unidirezionale e non consente all'utente di autenticare l'identità del BBS a cui sta' cercando di accedere.
Per consentire all'utente di autenticare il BBS sarebbe necessario eseguire la procedura di autenticazione soprascritta anche nel verso contrario all'atto delle connessione in questo modo:

L'utente X chiama il BBS Y.
Il BBS Y risponde.
L'utente X chiede al BBS Y di verificare la sua identità inviando un challenge.
Il BBS dovrà rispondere inviando il challenge elaborato con MD2 e codificato con la sua chiave privata. L'utente sarà certo dell'identità del BBS solo se decodificando la risposta con la chiave pubblica del BBS, questa coinciderà al challenge inviato e codificato con MD2.

Questa e' realizzabile in pratica solo utilizzando una procedura automatizzata in uno script file, in quanto a un utente privo di conoscenza specifica diventerebbe troppo complessa da gestire.

Una proposta di standardizzazione per il prompt di richiesta di autenticazione

Sebbene gran parte dei programmi che forniscono un metodo per automatizzare l'invio della password sono in grado di discriminare senza problemi i diversi tipi di **challenge** credo sia importante standardizzare il prompt di richiesta della password con un header comune.
Il prompt proposto e' fatto nel seguente modo:

RICHIESTA_VERBALE <NOMINATIVO_BBS:PROTOCOLLI> **challenge** challenge1….

Dove:

DI_RICHIESTA_VERBALE	=	? Password
NOMINATIVO_BBS	=	IW3FQG

PROTOCOLLI:

N5	=	NETROM a 5 caratteri
MD2	=	MD2
RSA128	=	RSA con chiavi asimmetriche lunghe 128 bit

Es.

? Password <IW3FQG:N5-MD2-RSA128> 1 2 3 4 5 [0123456789]

Uno sguardo all'algoritmo RSA

L'algoritmo di cifratura RSA, dal nome degli inventori (Ron L. Rivest, Adi Shamir e Leonard M. Adleman), fu pubblicato per la prima volta nel 1978 (cfr. pp. 120-126 di Communication of the ACM v.21 n.2 Febbraio 1978) impiega una coppia di chiavi asimmetriche una pubblica (che può essere facilmente fatta circolare) e una privata che resta segreta.
Gli impieghi di questo algoritmo sono molteplici, si va' dallo scambio di file cifrati attraverso un canale insicuro senza bisogno che i due corrispondenti si scambino la password di cifratura, fino a realizzare un protocollo di autenticazione sicuro attraverso un canale di comunicazione insicuro.
La conoscenza della nostra chiave pubblica consente a chiunque di verificare la nostra identità ma in nessun modo di risalire alla nostra chiave privata.
L'algoritmo basa la sua sicurezza sulla difficoltà di fattorizzare un numero molto grande (100~200 o più cifre), in altre parole la sua scomposizione in una coppia di numero primi. Riuscire a trovare i 2 numeri primi che compongono un numero a molte cifre, e' un'operazione abbastanza lunga, al contrario quando si conoscono i 2 fattori il calcolo del prodotto richiede sono alcuni secondi (frazioni di secondo se si tratta di un computer).

La costruzione delle chiavi avviene seguendo i passi che seguono:

Per la chiave pubblica:
1. Si scelgono due numeri primi detti p e q (che devono rimanere segreti) e si calcola il loro prodotto n =pq
2. Si sceglie un numero detto e che sia primo rispetto a p-1 e q-1

Per la chiave privata:
1. Si calcola un numero detto d tale che ed =1 **mod** (p-1)(q-1)

La chiave pubblica e' composta dalla coppia: **e,n**
La chiave privata e' composta dalla coppia: **d,n**

La funzione di trasferimento per la codifica: m^e **mod** n
La funzione di trasferimento per la decodifica: c^d **mod** n

L'implementazione

Le implementazioni di tutti i protocolli descritti nel presente testo e' stata realizzata a più riprese negli anni dal sottoscritto e altri colleghi radioamatori italiani e stranieri.

In questo momento i programmi realizzati dal sottoscritto che implementano l'algoritmo RSA sono:

- Per i BBS F6FBB versione 7.xx (DOS/WIN) e' disponibile il software GETPASS v7.0 che funziona come add-on C_FILTER.DLL
- Per gli utenti che utilizzano terminali in text mode e operano in MSDOS software SENDPASS v4.0
- Per gli utenti che utilizzano terminali in Windows il software SENDPASS for Windows v4.0 (non ancora disponibile) in formato standalone, DLL e ActiveX

Infine ricordo che il software SENDPASS fornisce il supporto oltre che per generare le password per i BBS anche per accedere in modalità supervisore ai nodi FLEXNET, G8BPQ, ITANET, NETROM/TheNet e SuperVozelj.

Aprile 1998.

Marco IW3FQG

packet-radio: iw3fqg@i3kuh.iven.ita.eu
email: msave@tin.it