


Falso senso di sicurezza: le serrature Master-Keyed

a cura di
Attilio Stanziale

Sistemi di Elaborazione dell'Informazione
(Sicurezza su Reti)

Prof. Alfredo De Santis

INDICE

- Introduzione 
- Le Serrature Meccaniche
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco
 - Contromisure
- Pubblicazione del Lavoro
- Conclusioni


Introduzione

Per aprire una serratura chiusa a chiave spesso non è necessario scassinarla:
basta sfruttare le sue vulnerabilità...



Vedremo una tecnica per un tipo di serratura "*a passe-par-tout*", le serrature **Master-Keyed**: un attacco trial and error permette di creare una master key che aprirà tutte le serrature del sistema

INDICE

- Introduzione
- Le Serrature Meccaniche 
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco
 - Contromisure
- Pubblicazione del Lavoro
- Conclusioni

Le Serrature Meccaniche


Per capire come funziona la tecnica che utilizzeremo, dobbiamo fare un passo indietro e studiare il funzionamento delle serrature meccaniche.



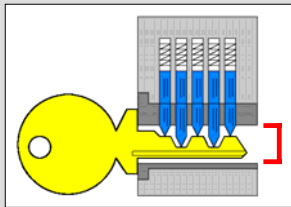
Vedremo:

- le serrature Pin Tumbler
- le serrature Master-Keyed

INDICE

- Introduzione
- Le Serrature Meccaniche 
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco
 - Contromisure
- Pubblicazione del Lavoro
- Conclusioni

Le Serrature Pin Tumbler (1)

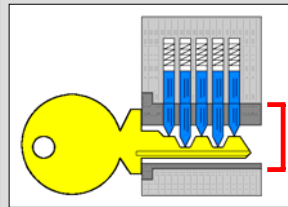


Sezione longitudinale di una serratura Pin Tumbler.

Disegno originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

- In queste serrature la chiave viene inserita in una fessura detta **keyway**.

Le Serrature Pin Tumbler (2)

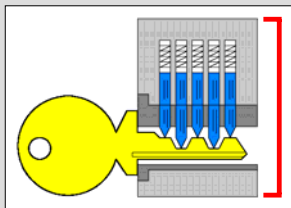


Sezione longitudinale di una serratura Pin Tumbler.

Disegno originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

- La keyway si trova su un cilindro mobile detto **plug**.

Le Serrature Pin Tumbler (3)

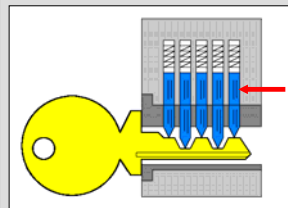


Sezione longitudinale di una serratura Pin Tumbler.

Disegno originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

- Il plug si innesta in un altro cilindro fissato alla porta, la **shell**.

Le Serrature Pin Tumbler (4)

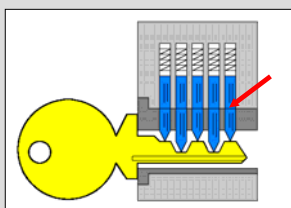


Sezione longitudinale di una serratura Pin Tumbler.

Disegno originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

- La shell ha dei fori dai quali sporgono dei **pin** spinti da molle, che si infilano nei corrispondenti fori del plug.

Le Serrature Pin Tumbler (5)



Sezione longitudinale di una serratura Pin Tumbler.

Disegno originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

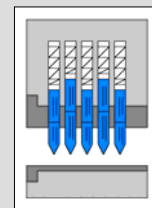
- Ogni pin è diviso in due da un **taglio** perpendicolare alla sua lunghezza.

Le Serrature Pin Tumbler (6)



NON INSERITA

tutti i tagli dei pin si trovano all'interno del plug che quindi non può ruotare



Sezione longitudinale di una serratura Pin Tumbler.

Disegno originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

Le Serrature Pin Tumbler (7)

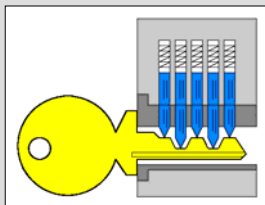


INSERITA

le tacche della chiave spingono i pin contrastando la forza delle molle

GIUSTA

tutti i tagli dei pin si allineano col bordo del plug (**shear line**), che libero di ruotare, aprirà la serratura



Sezione longitudinale di una serratura Pin Tumbler.

Diseño originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

Le Serrature Pin Tumbler (8)

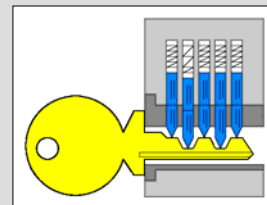


INSERITA

le tacche della chiave spingono i pin contrastando la forza delle molle

SBAGLIATA

qualche taglio non è allineato ed impedirà al plug di ruotare



Sezione longitudinale di una serratura Pin Tumbler.

Diseño originale: Copyright 1987, 1991 Theodore T. Tool. Tutti i diritti riservati.

Le Serrature Pin Tumbler (9)

Le profondità di tutte le tacche della chiave (**bitting**) rappresentano il "**segreto**" per aprire la serratura.




Le profondità hanno valori standard, quindi il bitting si può descrivere in modo conciso con i numeri interi (es. "12345").

Le serrature comuni hanno 4-7 pin, e 4-10 profondità distinte per le tacche: il numero di possibili chiavi va da 4^4 a 10^7 , abbastanza per impedire un attacco di forza bruta.





INDICE

- Introduzione
- Le Serrature Meccaniche
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed 
- Dedurre la Master Key
 - L'Attacco
 - Contromisure
- Pubblicazione del Lavoro
- Conclusioni

Le Serrature Master-Keyed (1)

Sono una variante delle serrature Pin Tumbler ed utilizzano due chiavi:

- **change key**  che apre solo una determinata serratura

- **master key**  che ne apre gruppi o tutte (in un sistema)

Le Serrature Master-Keyed (2)

tutti o alcuni pin hanno due tagli



la serratura ammette un ulteriore bitting

MASTER KEY

CHANGE KEY

bitting comune a più serrature


bitting specifico per una serratura

Le Serrature Master-Keyed (3)

Esistono due schemi per il bitting:

- **Total Position Progression**, ogni pin ha un taglio dedicato alla master key
- **Rotating Constant**, ogni change key condivide con la master key un certo numero di tagli, che varia (ruota) in ogni serratura

INDICE

- Introduzione
- Le Serrature Meccaniche
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco 
 - Contromisure
- Pubblicazione del Lavoro
- Conclusioni

L'Attacco (1)

Esistono varie tecniche per ottenere indebitamente una copia di una master key...

...ma ognuna ha degli svantaggi e dei limiti:

L'Attacco (2)

alcune richiedono la **visione della master key**...



...ma non è sempre possibile

L'Attacco (3)

oltre il **disassemblaggio della serratura** per studiarne i pin...



...ma si corre il rischio di essere scoperti

L'Attacco (4)

oltre lo studio di un **numero abbastanza grande di change keys** dello stesso sistema...



...ma non sempre è facile procurarsele e comunque non funziona con le serrature **"Rotating Constant"**

L'Attacco (5)

oppure tentare un **attacco di forza bruta**...



...richiede **D^p** test delle chiavi, irrealizzabile
D = numero di profondità delle tacche
P = numero di pin della serratura

L'Attacco (6)

il nostro attacco invece non ha inconvenienti e genera un **rights amplification non autorizzato**

partiamo da una **change key**



produciamo illegalmente una **master key**

otteniamo più privilegi di quelli che ci spetterebbero

L'Attacco (7)

Per il nostro attacco abbiamo bisogno di:

- una **change key**
- la **serratura** corrispondente
- alcune **chiavi vergini**
- uno strumento per inciderle (basta una **lima** per ferro)

L'Attacco (8)

useremo la serratura come un **“oracolo”**

accettando o rifiutando le chiavi fornisce informazioni sui singoli pin



L'Attacco (9)

PROBLEMA



La serratura si apre solo se i tagli di tutti i pin si allineano alla shear line:

otteniamo informazioni sull'intero bitting e non sui singoli pin.



L'Attacco (10)

SOLUZIONE



Sfruttiamo una debolezza delle serrature Master-Keyed:

i bitting formati da alcune profondità della change key e altre della master key apriranno la serratura.



change key = “11111” master key = “44444”
ma anche “14111”, “11411”, “11141”, ecc. ($2^{\#PIN}$ combinazioni)

L'Attacco (11)

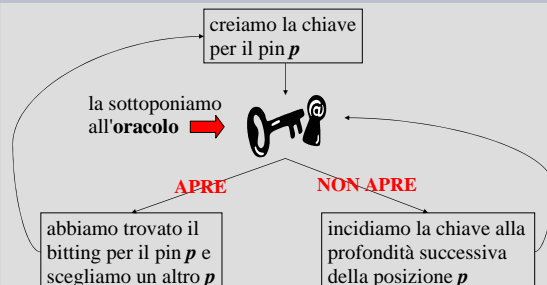
Sia P il numero di pin della serratura e sia D il numero di profondità distinte.



Creiamo una chiave identica alla change key tranne che nella posizione p , con p da 1 a P .

Nella posizione p avrà la profondità minore possibile (la tacca è più alta).

L'Attacco (12)



L'Attacco (13)

▪ **Total Position Progression:** la master key ha tagli dedicati, quindi per ogni pin troveremo sempre un'altra chiave che apre la serratura.

▪ **Rotating Constant:** alcuni tagli coincidono per change key e master key, in tal caso per quel pin non ci sarà un'altra chiave che apre.


L'Attacco (14)

Una volta determinati i bitting di ogni pin possiamo creare la nostra master key.



L'attacco richiede P chiavi vergini e nel caso peggiore $P \cdot (D-1)$ test delle chiavi. L'attacco di forza bruta ne richiede D^P !

INDICE

- Introduzione
- Le Serrature Meccaniche
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco
 - Contromisure 
- Pubblicazione del Lavoro
- Conclusioni

Contromisure (1)

Non ci sono soluzioni per eliminare questo attacco senza sostituire le serrature Master-Keyed, possiamo solo renderlo più difficile:


- usare serrature "a passe-par-tout" alternative (es. Master Ring, ma hanno altri difetti)
- usare serrature per cui sia difficile trovare chiavi vergini (possono sempre essere prodotte)
- aggiungere "falsi" tagli ad alcuni pin per confondere l'attaccante (è più vulnerabile verso altri tipi di attacchi)

Contromisure (2)

Gli esperti della **ALOA** (Associated Locksmiths of America) propongono anche altri accorgimenti:

- le serrature delle porte esterne degli edifici non devono essere Master-Keyed
- le zone più importanti non devono avere serrature Master-Keyed
- usare master key diverse per ogni piano o ala degli edifici
- nei condomini gli appartamenti non devono avere serrature Master-Keyed
- la master key non deve mai lasciare l'edificio

INDICE

- Introduzione
- Le Serrature Meccaniche
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco
 - Contromisure
- Pubblicazione del Lavoro 
- Conclusioni

Pubblicazione del Lavoro (1)

Questa vulnerabilità è venuta alla luce grazie ad un lavoro del professore Matt Blaze dell'Università della Pennsylvania.

La tecnica non è nuova (su internet ci sono attacchi simili) ma Blaze è stato il primo a studiarla in modo rigoroso.

Dopo la ri-scoperta Blaze mandò il lavoro a tutte le autorità americane e ad altri colleghi.

Alcuni dettagli arrivarono ad un reporter del New York Times che ci scrisse su un articolo.

Non potendo più nascondere il lavoro, decise di pubblicarlo.

Pubblicazione del Lavoro (2)

Dopo l'articolo del New York Times, Blaze ricevette numerose lamentele dai produttori di serrature:

"tutti gli addetti ai lavori già conoscevano l'attacco e ora lo conoscono anche i malintenzionati"

ma anche commenti positivi da esperti di sicurezza industriale che non lo conoscevano.

Pubblicazione del Lavoro (3)

Questo dimostra che nel mondo delle serrature è in vigore la nozione del **"security through obscurity"**: mantenere segrete le informazioni per non dare vantaggi agli attaccanti.

Il suo opposto (diffuso in informatica) è la **"full disclosure"**: rendere pubblici i dettagli per permettere agli esperti di analizzarli ed evidenziarne i difetti (*"peer review"*).


Pubblicazione del Lavoro (4)

La full disclosure deriva dalla **"legge di Kerckhoffs"**:

"un sistema crittografico dovrebbe essere sicuro anche se ogni cosa che riguarda il sistema, ad eccezione della chiave, è di pubblico dominio".

Per le serrature, è facile ottenere un modello da studiare per trovare delle vulnerabilità, quindi la sicurezza da **"oscurità"** verrà meno inevitabilmente.

INDICE

- Introduzione
- Le Serrature Meccaniche
 - Le Serrature Pin Tumbler
 - Le Serrature Master-Keyed
- Dedurre la Master Key
 - L'Attacco
 - Contromisure
- Pubblicazione del Lavoro
- Conclusioni 

Conclusioni (1)

L'attacco ha notevoli implicazioni sulla sicurezza: queste serrature sono le più diffuse in uffici, scuole, università, complessi residenziali, ecc.

La tecnica presentata non lascia segni di effrazione, non richiede particolari abilità, ed utilizza solo qualche chiave vergine ed una lima per ferro.

Inoltre, l'attaccante non avrà comportamenti sospetti (utilizza solo la propria serratura) e può effettuare l'attacco, che di solito richiede pochi minuti, anche in più sessioni.

Conclusioni (2)

la vulnerabilità deriva dal fatto che possiamo ottenere **informazioni sui singoli pin**



l'attacco richiede **tempo lineare** rispetto al numero dei pin, invece che esponenziale



dal punto di vista crittografico, le serrature Master-Keyed sono **irrimediabilmente insicure** e non dovrebbero essere utilizzate