Analisi Sicurezza Serrature

Alfredo De Santis
Dipartimento di Informatica
Università di Salerno

ads@dia.unisa.it
http://www.dia.unisa.it/professori/ads

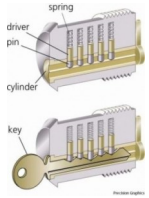
Marzo 2014

Analisi sicurezza

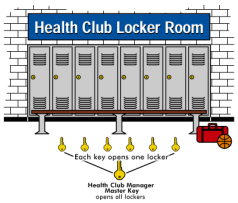
- Necessario grandi spazi per possibili chiavi private
- Evitare vulnerabilità dei sistemi

- Analizziamo queste problematiche
  - Caso di studio: le serrature

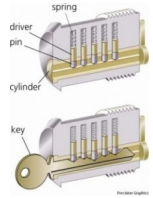
Sommario



- Serrature Pin Tumbler
- Serrature Master-Keyed
  - Vulnerabilità
  - Attacco
  - Contromisure



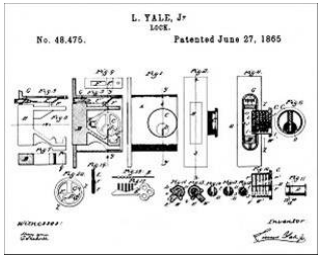
Sommario



- Serrature Pin Tumbler
- Serrature Master-Keyed
  - Vulnerabilità
  - Attacco
  - Contromisure

Cilindro con chiave

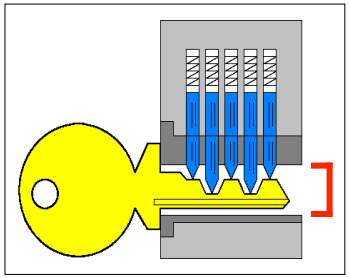
Il cilindro con chiave fu inventato da Linus Yale, Sr., nel 1848
Il figlio Linus Yale, Jr., lo migliorò (chiavi più piccole e piatte) e lo brevettò nel 1861



Altro brevetto registrato nel 1865

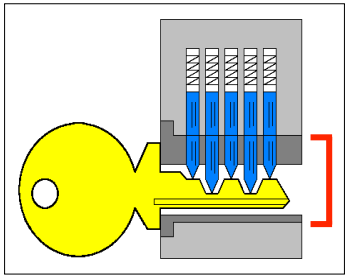
Uno dei primi cilindri Yale

Le Serrature Pin Tumbler (1)



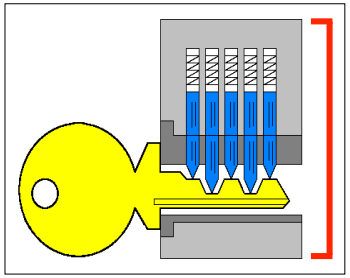
la chiave viene inserita in una fessura detta keyway

Le Serrature Pin Tumbler (2)



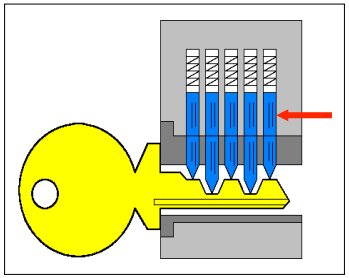
La keyway si trova su un cilindro mobile detto plug

Le Serrature Pin Tumbler (3)



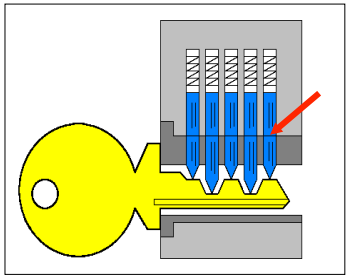
Il plug si innesta in un altro cilindro fissato alla porta, la shell

Le Serrature Pin Tumbler (4)



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)

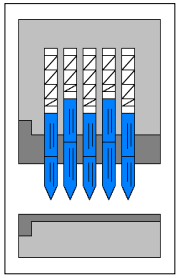


Ogni pin è diviso in due da un taglio perpendicolare alla sua lunghezza

Le Serrature Pin Tumbler (6)

Chiave non inserita

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

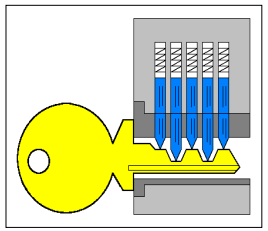


Le Serrature Pin Tumbler (7)

Chiave inserita

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

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

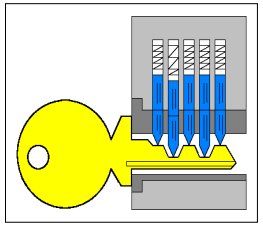


Le Serrature Pin Tumbler (8)

Altra chiave inserita

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

qualche taglio non è allineato ed impedirà al plug di ruotare



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.

Complessità attacco "forza bruta"

- Se si provasse 1 chiave ogni 5 secondi occorrono
  - 4^4 x 5 secondi = 1.280 secondi ≈ 21 minuti
  - 10^7 x 5 secondi ≈ 1 anno 213 giorni

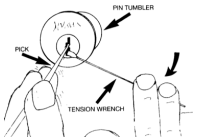
  nel caso peggiore (nel caso medio, la metà)

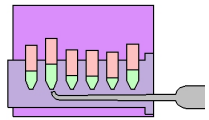
- Alcuni numeri di riferimento:
  - Secondi in un ora 60 x 60 = 360
  - Secondi in un giorno 360 x 24 = 86.400
  - Secondi in un anno 86.400 x 365 = 31.536.000

Le Serrature Pin Tumbler (10)

Lock picking - grimaldelli

tool …





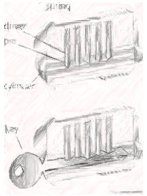
Using a hook pick to feel for the binding pin

Le Serrature Pin Tumbler (11)

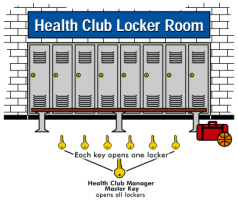
Lock picking

libri …

Sommario



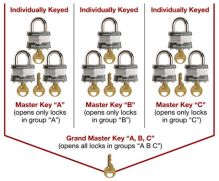
- Serrature Pin Tumbler
- Serrature Master-Keyed
  - Vulnerabilità
  - Attacco
  - Contromisure

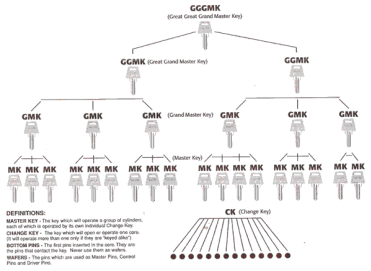


Serrature Master-Keyed (1)

Cosa sono?

(dette anche passepartou)

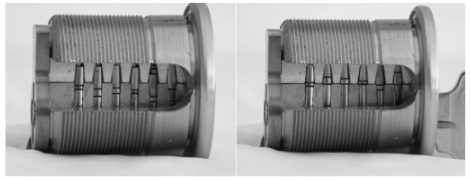




Serrature Master-Keyed (2)

Consideriamo il caso:

Una sola *master key* e diverse *change key*



Tutti i pin (o alcuni) hanno 2 tagli:

Uno per la master key e l'altro per la change key

Serrature Master-Keyed (3)

Vari tipi di attacchi:

- Visione della master key
- Disassemblaggio serratura e studio

  Si può essere scoperti
- Studio di un gran numero di change key

  Non facile procurarsele
- Attacco di forza bruta

  richiede D^P (D profondità tacche, P numero pin)

Serrature Master-Keyed (4)

Descriviamo un attacco di rights amplification

Occorrente:

- Una change key
- Serratura corrispondente
- P chiavi vergini
- Strumento per inciderle (basta una lima per ferro)

Idea:

- Usa la serratura come oracolo
- Partire con chiave vergine e limare poco alla volta fino ad ottenere il bitting per ogni pin

Serrature Master-Keyed (5)

Vulnerabilità sfruttata:

- Non ci sono solo 2 bitting che aprono la serratura
- Supponiamo change key ="11111" master key="44444"
- Allora 2^5 combinazioni aprono la serratura, cioè "14111", 11411", "11141", …

Serrature Master-Keyed (6)

Attacco:

```
for p=1 to P
   for d=1 to D
      Creare chiave identica alla change key,
      eccetto in posizione p dove la tacca è limata a profondità d.
      Se la chiave apre, allora d è un bitting per il pin p.
```

Serrature Master-Keyed (7)


Attacco:

for p=1 **to** P
  for d=1 **to** D
    Creare chiave identica alla change key,
    eccetto in posizione p dove la tacca è limata a profondità d.
    Se la chiave apre, allora d è un bitting per il pin p.

Complessità :
- Numero chiavi vergini usate P
- Numero test necessari P(D-1) nel caso peggiore

Altro vantaggio attacco: non lascia segni di effrazione

Serrature Master-Keyed (8)

Insegnamento:
- Una vulnerabilità ci ha consentito di ottenere informazioni sui singoli pin
- Da un attacco esponenziale D^P siamo arrivati ad un efficiente P(D-1)

Serrature Master-Keyed (9)

Contromisure:
- Analisi rischi per serraure master keyed
  - Eliminarle oppure conservarle? Installarle o no?
- Usare serrature per cui è difficile trovare chiavi vergini
- Separare uso delle master keyed:
  diversi sottogruppi di una organizzazione hanno diverse ed indipendenti sistemi master keyed.

Bibliografia

Matt Blaze,
Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks,
IEEE Security and Privacy, 2003

Matt Blaze,
Keep it secret, stupid!
http://www.crypto.com/papers/kiss.html

Divulgazione vulnerabilità

- New York Times, gennaio 2003
- Molte proteste dai costruttori
- Vulnerabilità era già conosciuta dai costruttori da decenni
  - Ma non diffusa, nemmeno ai clienti
  - Anche usata qualche volta per recupero master key perse da clienti


The New York Times

Business Day

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search

Global | DealBook | Markets | Economy | Energy | Media | Personal Tech | Small Business | Your

Master Key Copying Revealed

By JOHN SCHWARTZ
Published: January 23, 2003

A security researcher has revealed a little-known vulnerability in many locks that lets a person create a copy of the master key for an entire building by starting with any key from that building.

The researcher, Matt Blaze of AT&T Labs-Research, found the vulnerability by applying his area of expertise — the security flaws that allow hackers to break into computer networks — to the real-world locks and keys that have been used for more than a century in office buildings, college campuses and some residential complexes.

SIGN IN TO E-MAIL
PRINT
SINGLE-PAGE

SOUND OF MY VOICE
IN THEATERS AT CAMPUS

Click to View

Divulgazione vulnerabilità

- Ci sono architetture alternative per le master key, che non hanno questa vulnerabilità, ma non sono state sviluppate dai costruttori
- "…a story that Richard Feynman famously told about his days on the Manhattan project. Some simple vulnerabilities (and user interface problems) made it easy to open most of the safes in use at Los Alamos. He eventually demonstrated the problem to the Army officials in charge. Horrified, they promised to do something about it. The response? A memo ordering the staff to keep Feynman away from their safes."

Domande?