Lockpickito
ergo sum

Walter Belgers
walter@ehv.toool.nl

About me

• Walter Belgers
• Partner, Principal Security Consultant at Madison Gurkha (Netherlands) (penetration testing, social engineering, etc)

Outline

LOCKS!

Opening a lock

• Normal entry
  • Using the key and/or codes
• Forced entry
  • Using destructive techniques
• Covert/surreptitious entry
  • Not leaving obvious traces

Forced entry

• Attacking not the locking mechanism itself
Forced entry, protection

Covert/surreptitious entry
- Opening a lock without using the key/knowing the correct code
- Without breaking the lock
- Without leaving (obvious) traces behind
- Traces may be found upon close examination

Lockpicking
“The sport of opening locks covertly, with permission of the owner.”

Copying the key
- Of course, if you have the key, you can copy it

Copying the key

http://www.quick-key.de/
Copying the key

Lockpicking

- Understand how a lock works
- Think of ways to circumvent security

- This is actually “hacking”
- Circumventing security by thinking out of the box

Alignment of plug holes

- Misalignment of plug holes makes it possible to open a lock by lifting the pins one at a time
- Mechanical/economical limitation
Lockpicking

- This technique works with:
  - Pin-tumbler locks (including padlocks)
  - Wafer tumbler locks
  - Dimple locks
  - Tubular locks

Dimple locks

Raking: a shortcut

- Using a technique called raking, we can try to set more than one pin at the same time
- With cheap locks, raking is all that is needed to open them
- With better locks, raking can still be useful
  - Rake 2, 3, 4 pins
  - Set the last one(s) using standard picking techniques

Raking tools

Countermeasures

- Drilling and pulling:
  - Harder materials
  - Special pins
- Key duplication:
  - Certificates
  - Specially formed keys
  - Patents
Countermeasures

- Picking:
  - Mushroom pins
  - Awkward keyway
  - New design/technology

Mushroom pins

- Makes it harder (not impossible) to pick a lock
- Often just a few pins are mushroom pins

Spool pins

Tips

- Do not use too much pressure (both tensioner and pick)
- Do not use too much pressure
- Relax and do not use too much pressure
- When it doesn’t work, reset and try again, but with less pressure
- Be sure that you are picking a lock that is not open already

Multiple systems

- Mul-T-Lock: pin-in-pin system
Multiple systems

- Abus/Pfaffenhain: multiple rows of pins
- Second row on the side
- Awkward keyway

Pick gun

- Different technique
- Transfer the energy like with billiard balls

Pick gun

Bumping

- Pick gun on steroids
- Use a key as “pick gun”, so awkward keyways are no problem (also works on dimple locks)
Kaba Quattro

GERA
- Magnet in the key pulls one pin up
- (Patent!)

Defeating bumping
- CES: bump key does not touch all pins

Rotating disc locks

SEA
Decoding

- Lockpicking, bumping, will open the lock only once
- Decoding is finding out what the key looks like
- And maybe opening at the same time

Decoding - Sputnik

Decoding - ABUS

Decoding - Impressioning
Locks can combine characteristics but must stay within space and money limitations.

- Lock manufacturer chooses from his bag of tricks to build a lock with certain characteristics w.r.t.:
  - Price
  - Key duplication and lock copying (patents)
  - Resistance to force, lockpicking, bumping, decoding
Workshop

- Tomorrow & the day after tomorrow
- Between 13:00 and 16:00 (give or take)
- BYOL (Bring Your Own Lock) if you like

Thanks!
walter@ehv.toool.nl