...Act as a motivating force in security designs and engineering.

VULNERABILITY ASSESSMENT OF COMMONLY AVAILABLE PERSONAL SAFETY BOXES IN THE PHILIPPINES

A presentation for RootCon 6 (September 2012)

By: JollyMongrel (aw! aw!)

Presentation outline

- Aim/s
- Literature review
- Materials & method
- Results & Discussion
- Case study & Simulation (video)
- Conclusion
- Summary & Recommendation
- References

Aim

- To evaluate weakness/es of commonly available personal safety box/es in the Philippines.

Literature Review

- Safe depository defined
  - A specially designed container for security providing resistance to penetration by forcible means.
- History of safes
  - While Egyptians & Greeks were the first to utilize vaults, the ancient Chinese and Romans kept their valuables in smaller chests.
  - Ancestry of modern safes are from locked metal-reinforced wooden boxes and chests (popular among pirates) in the medieval period.
  - 17th century: cast iron chests
  - 18th century: commercial safes were produced & sold in Great Britain.
  - 19th century: development of sophisticated safes to thwart technically adept burglars and to protect from fire.

Literature Review

- Protective mechanism of safes
  - Doors
    - Primary barrier for access
  - Boltworks
    - Complex mechanical boltwork are often integrated with relockers.
  - Booby trap
    - Legend of the Yamashita treasure chests rigged with booby-traps. Common booby traps are noxious gases that are engaged upon disturbance.
  - Glass plates
    - Mounted on sides. Breaking one of them would fire relockers installed.
  - Thermal buffers
    - These materials absorb and reduce surface temperature below melting point to prevent torching.
  - Relockers
    - Triggering them would permanently lock the safe

Literature Review

- Safecracking
  - Destructive
    - Drilling
    - Explosives
    - Torching
    - Impact
    - Prying
    - Peeling
    - Sawing, cutting, grinding
  - Non-destructive
    - Manipulation
    - Bypass
    - Guessing the combination

Literature Review

- Electronic Locks
- Override (tubular lock)
- Where are they installed?
  - Money safes
  - Gun safes
  - Document safes
  - Etc…
- Who prefers them?
  - Techie people
  - Oldies
  - Relatively busy people (Executive-like)

Materials & method

Equipment

- Electronic safe with tubular lock
- Homemade picks & bypass tool
- Stopwatch

Methodology

- Non-destructive method (surreptitous)
  - **Treatment 1:** Picking the bypass lock and retain the combination key
  - **Treatment 2:** Percussive bypass and retain the combination key
- Other methods were successfully tried but did not qualify as surreptitious such as button reset (*using thin plastic with thread as jimmy and a long stick to hit the reset button*) was not considered in this experiment.

Materials & method

- **Treatment 1:** A tubular pick made from available materials (hard tube, hairdressing pins and rubber bands) was used to pick the safe. Time was recorded for every successful opening (in three (3) replicates).

Materials & method

- **Treatment 1**

Materials & method

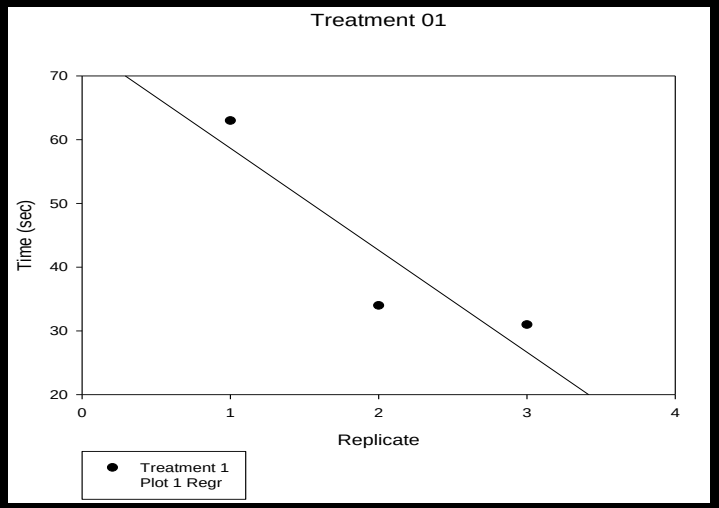
- **Treatment 2:** A blow from the top of the safe was delivered by hand. The energy generated from the blow (and the constant gravitational pull) pushes the solenoid below. With perfect timing and rotation of the knob/spindle, the safe was opened successfully. Time was then recorded for every successful opening (in three (3) replicates).

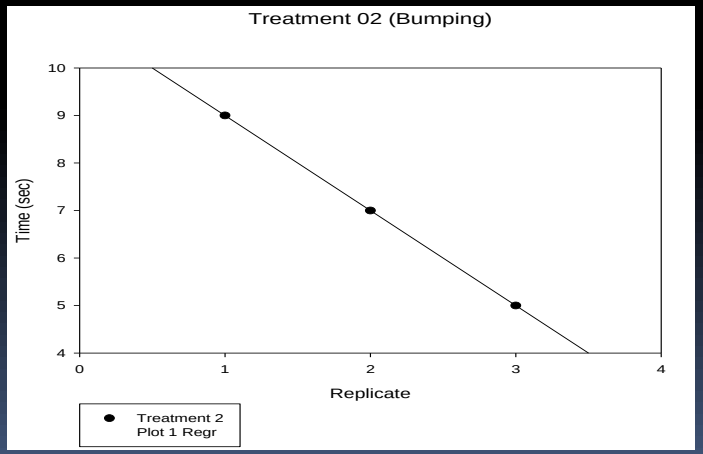
Materials & method

- **Treatment 2**

Results & discussion

- Treatment 1
  - R1 = 63sec
  - R2 = 34sec
  - R3 = 31sec
- Treatment 2
  - R1 = 9sec
  - R2 = 7sec
  - R3 = 5sec





Results & discussion

t-test Monday, September 03, 2012, 4:30:23 PM

Data source: Data 1 in Notebook1

Normality Test: Passed (P = 0.325)

Equal Variance Test: Passed (P = 0.394)

Group Name	N	Missing	Mean	Std Dev	SEM
Treatment 1	3	0	**42.667**	17.673	10.203
Treatment 2	3	0	**7.000**	2.000	1.155

Difference **35.667**

t = 3.473 with 4 degrees of freedom. (P = 0.026)

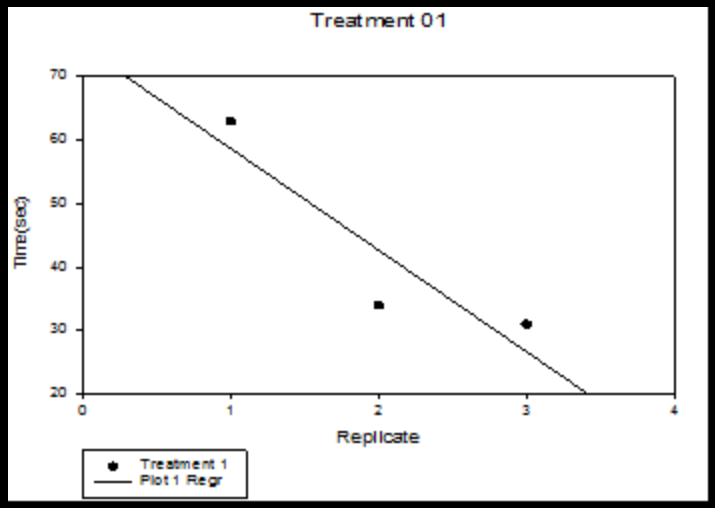
95 percent confidence interval for difference of means: 7.156 to 64.177

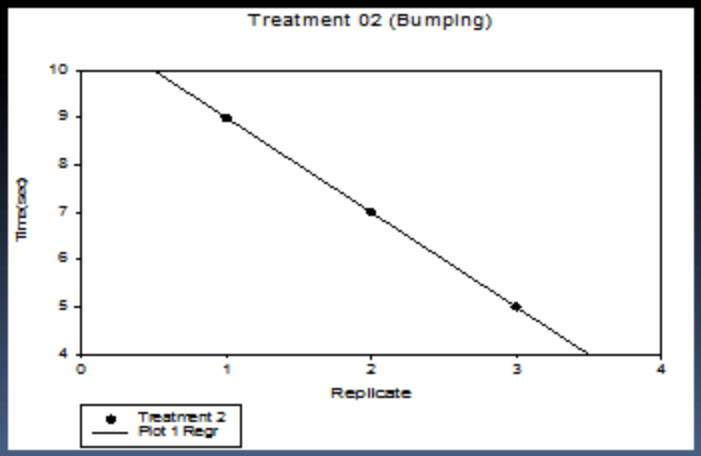
- **The difference in the mean values of the two groups is greater than would be expected by chance; there is a statistically significant difference between the input groups (P = 0.026).**

Power of performed test with alpha = 0.050: 0.708

Results & discussion

- The result suggest that treatment 2 opens the safe faster at mean time 7 sec, which is almost 6 times faster than treatment 1 at mean time 42 sec.
- Moreover, the linearity on both graph shows that at subsequent trials, the time to open decreases considerably.





Case study & Simulation

- Covert entry scenario (Teaser for the next Rootcon presentation)

Conclusion

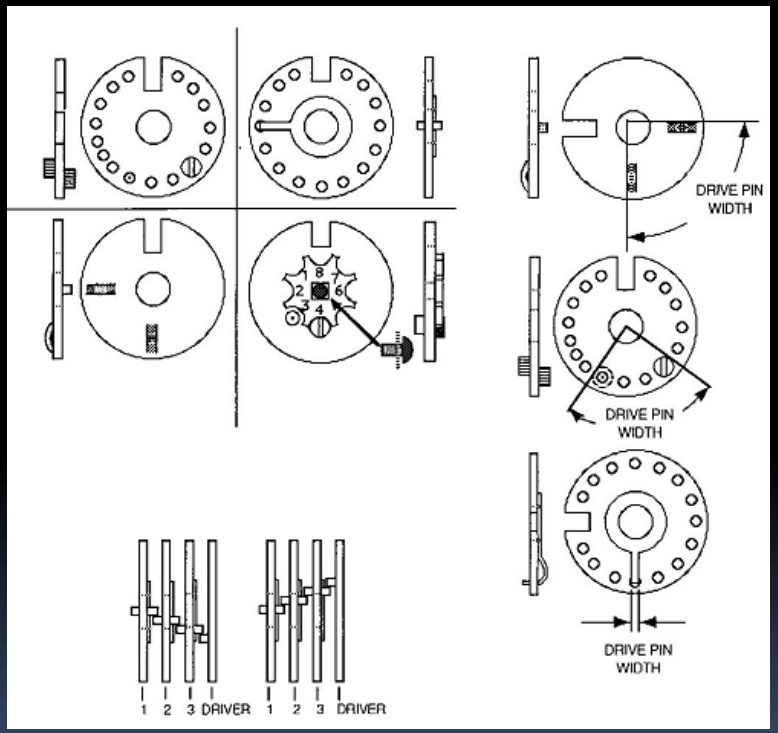
- Regardless of brand name, commonly sold electronic safes with solenoid drives and tubular lock override can be surreptitiously opened through percussive compromise or lockpicking.

Summary & Recommendation

- Aim/s
- Literature review
- Materials & method
- Results & Discussion
- Case study & Simulation (video)
- Conclusion
- Summary & Recommendation
- References

Possible future presentation (subject to availability of test materials)

- Manipulating mechanical combination locks.
- Impressioning



References

- LSS by Marc Tobias
- http://www.crypto.com/papers/safelocks.pdf
- http://www.timhunkin.com/
- http://www.safeman.org.uk/