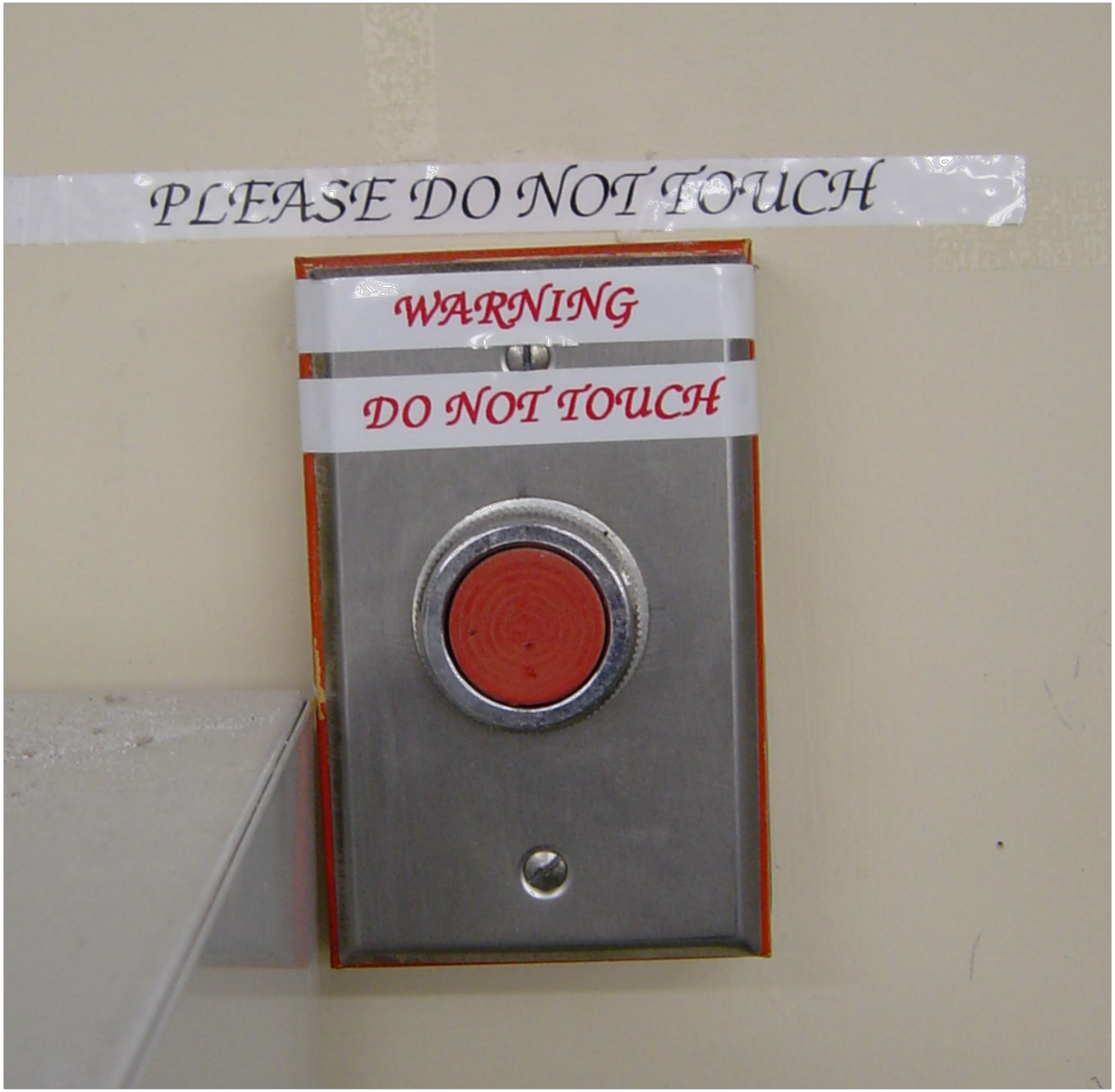
A conversation about

physical security

Mark Seiden, Internet Archive
mis@seiden.com, Dec 9, 2020

As a physical security tester, you see all kinds of things

- Physical security is not an abstraction
- Most buildings are not built *primarily* for security (a few exceptions: jails/prisons, missile silos, precious material vaults) — and even those are breached on a regular basis
- Even if they were built to be secure, 20 years later they are unlikely to be still secure


PLEASE DO NOT TOUCH
WARNING
DO NOT TOUCH

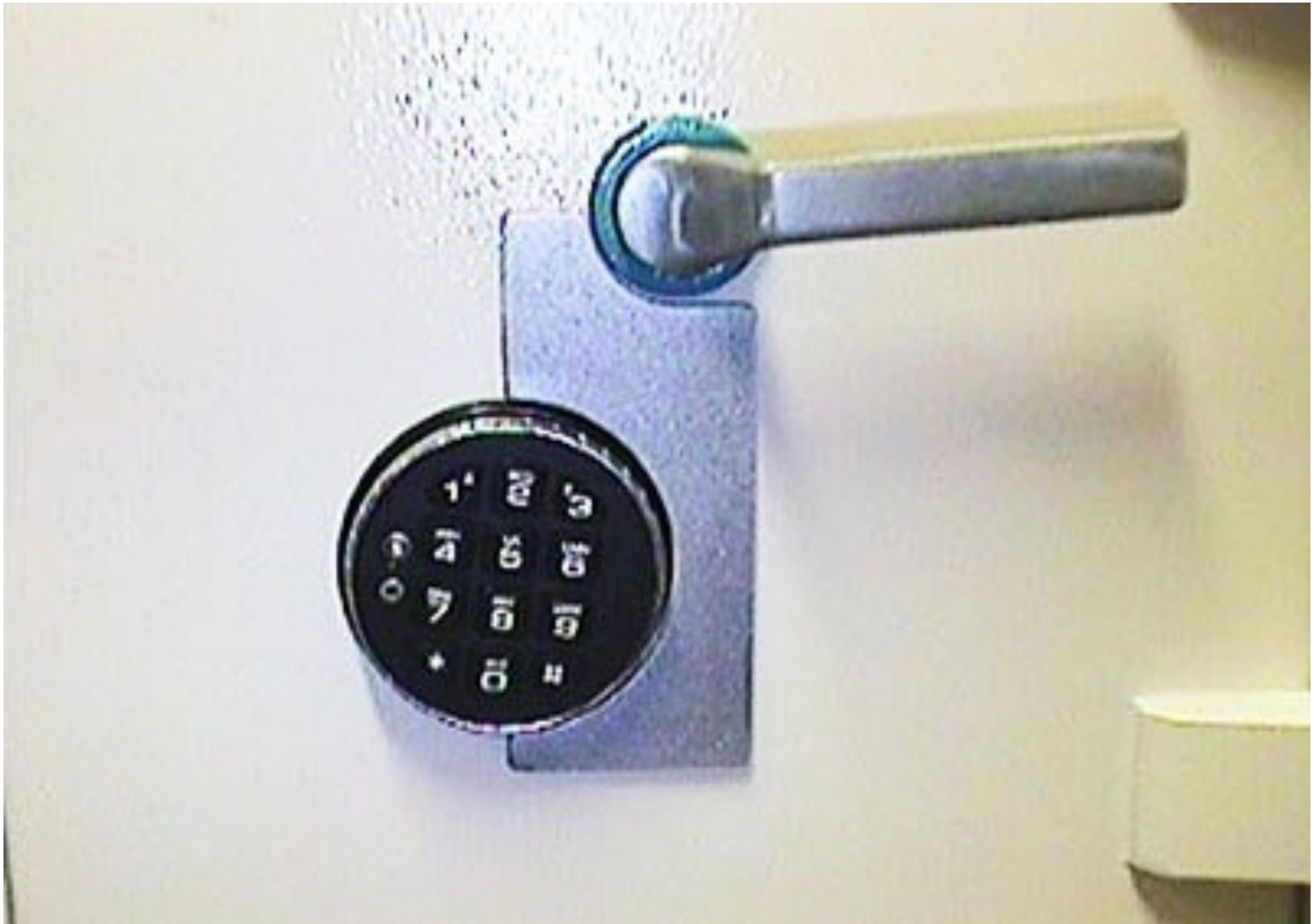
The assumptions change and technology improves

- Many of the proofs of concept and attacks here were first demonstrated more than 10 years ago!

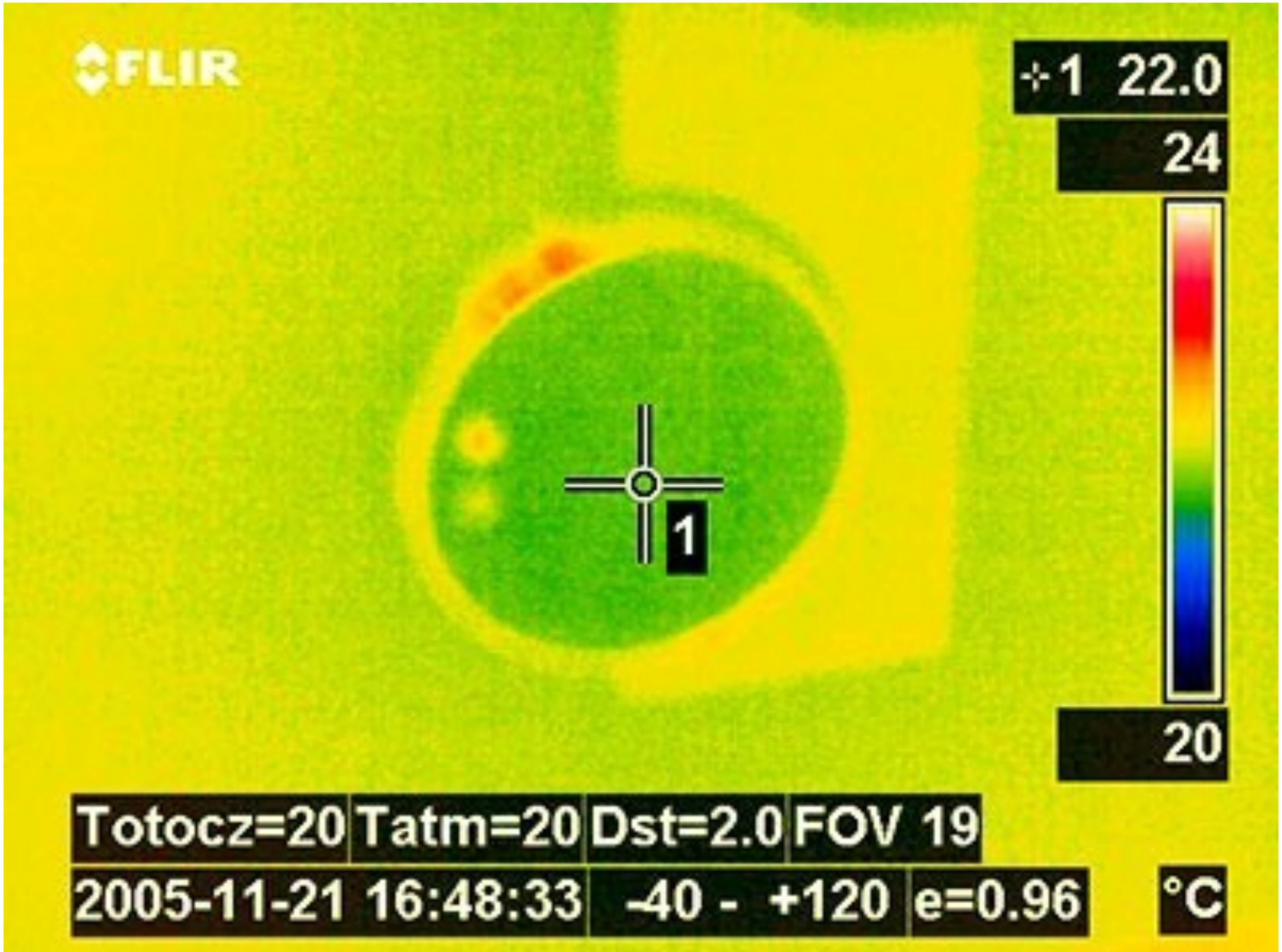
Cracking safes with thermal imaging (Zalewski,2005)

- A viable alternative to mind reading
- Handheld thermal imaging devices ($5k-10k new) have .05 degree K resolution. 1-10 meter range. Work up to 5-10 minutes after contact.
- “Whenever two objects come into contact, an exchange of material will occur” or “Every contact leaves a trace”- Edmond Locard, around 1910

The target

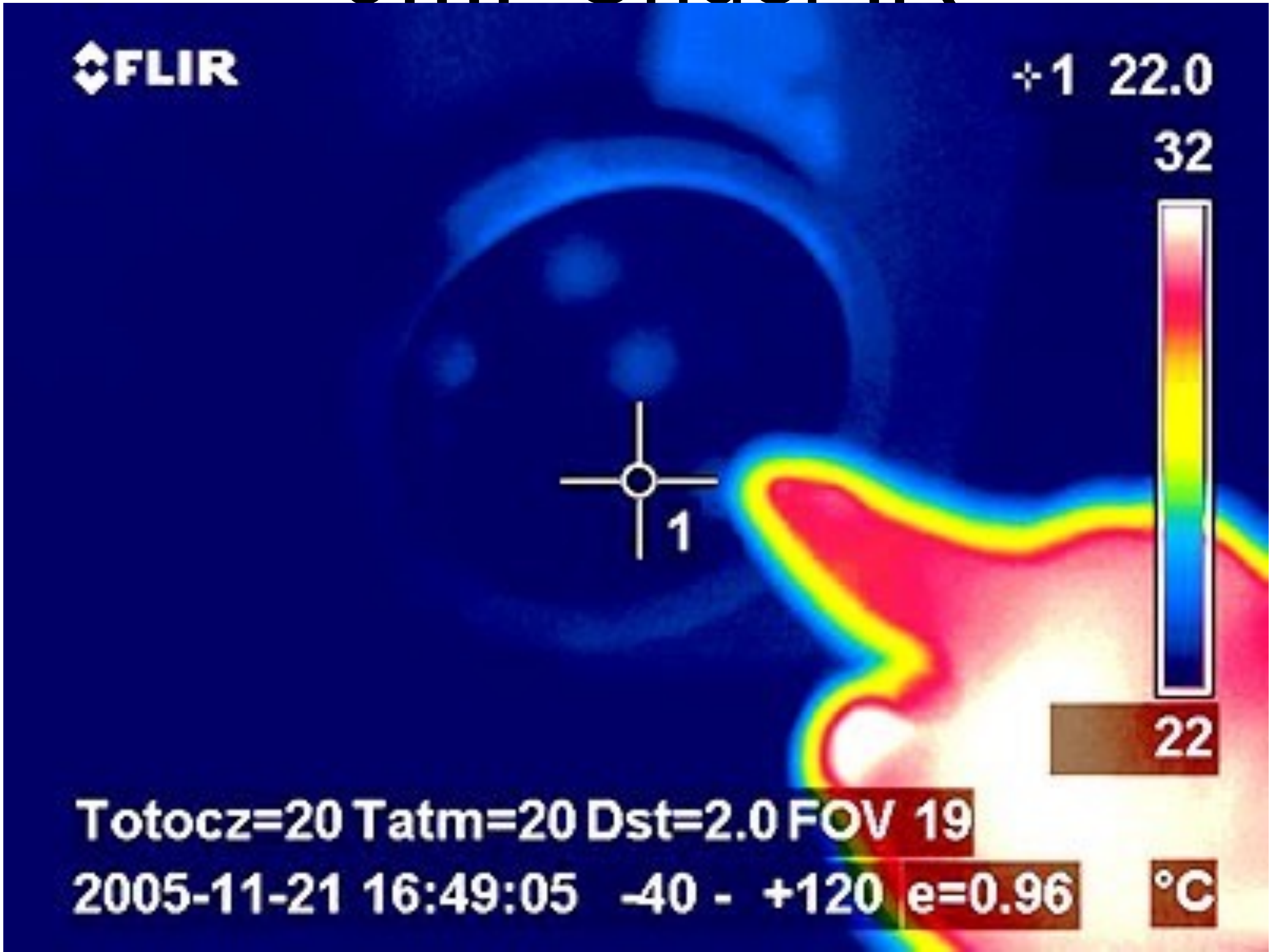


Under IR

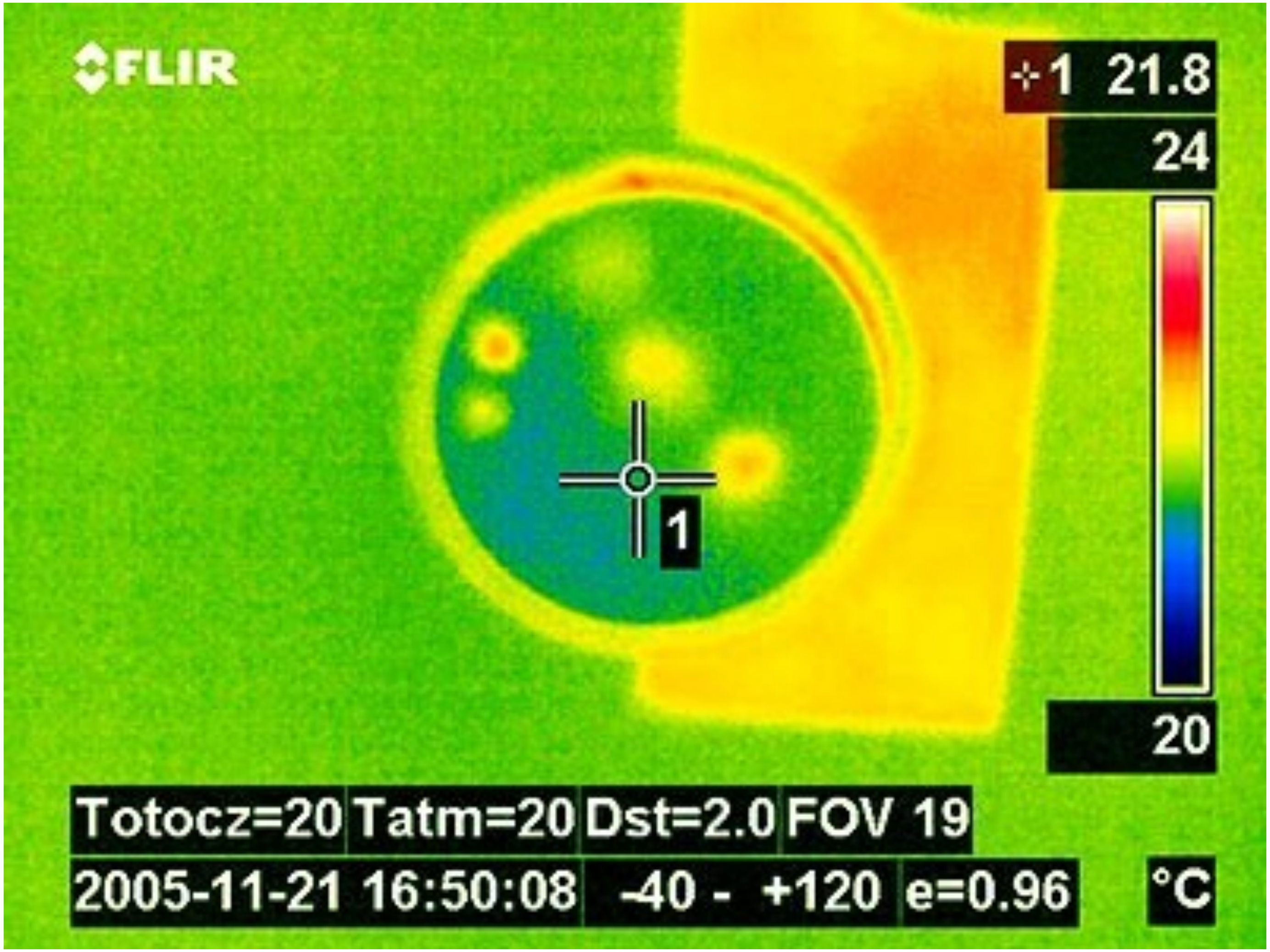

FLIR
1 22.0
24
1
20
Totocz=20 Tatm=20 Dst=2.0 FOV 19
2005-11-21 16:48:33 -40 - +120 e=0.96
°C

1, 5, …

9….. Under IR

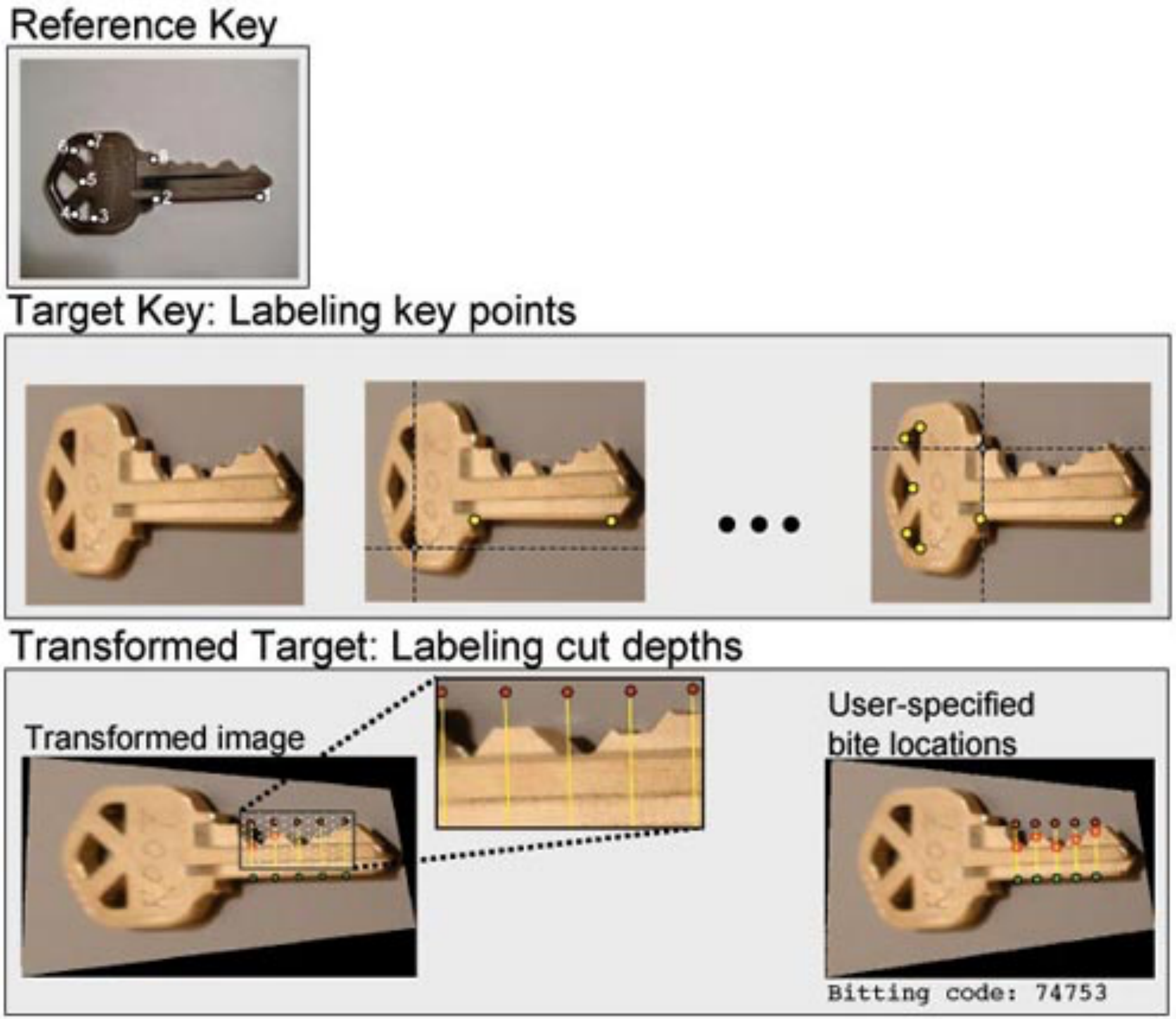

FLIR
1 22.0
32
1
22
Totocz=20 Tatm=20 Dst=2.0 FOV 19
2005-11-21 16:49:05 -40 - +120 e=0.96
°C

63 seconds later:


FLIR
1 21.8
24
20
1
Totocz=20 Tatm=20 Dst=2.0 FOV 19
2005-11-21 16:50:08 -40 - +120 e=0.96 °C

Laxton, Wang and Savage, “Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding”, ACM CCS 2008

http://vision.ucsd.edu/~blaxton/pageImages/top_pic.jpg



Reference Key

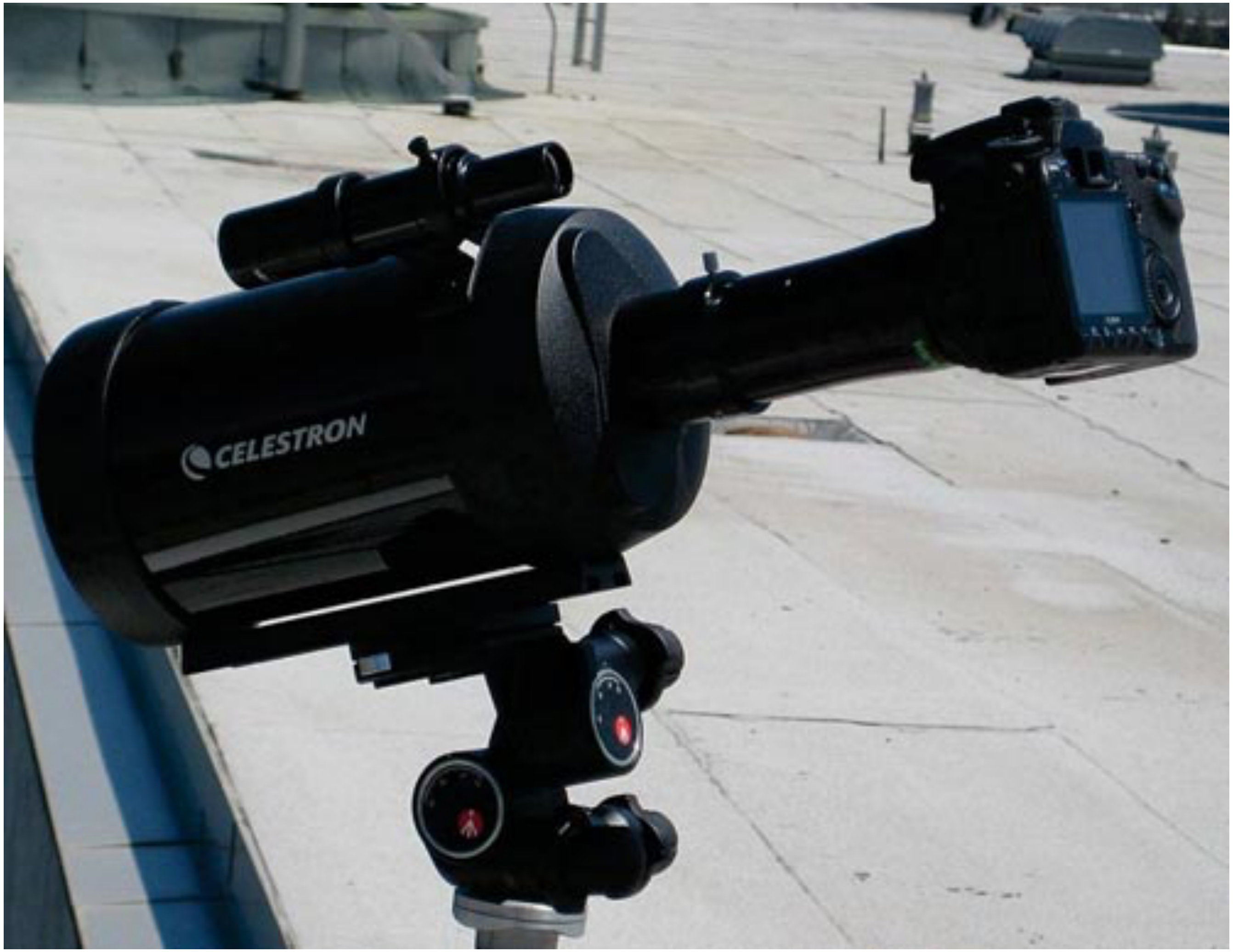
Target Key: Labeling key points

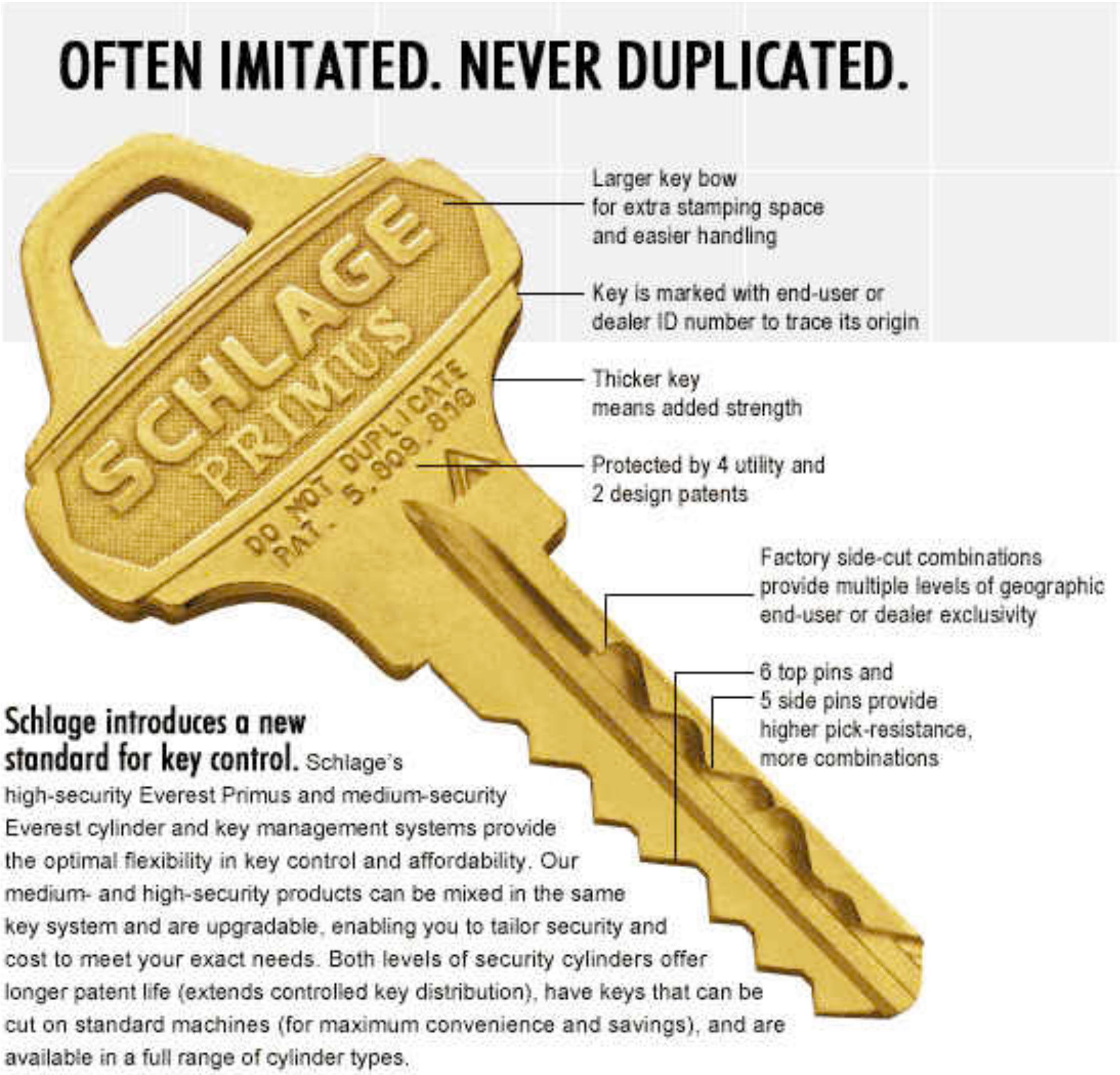
Transformed Target: Labeling cut depths

Transformed image

User-specified bite locations

Bitting code: 74753


CELESTRON



OFTEN IMITATED. NEVER DUPLICATED.

Larger key bow for extra stamping space and easier handling

Key is marked with end-user or dealer ID number to trace its origin

Thicker key means added strength

Protected by 4 utility and 2 design patents

Factory side-cut combinations provide multiple levels of geographic end-user or dealer exclusivity

6 top pins and 5 side pins provide higher pick-resistance, more combinations

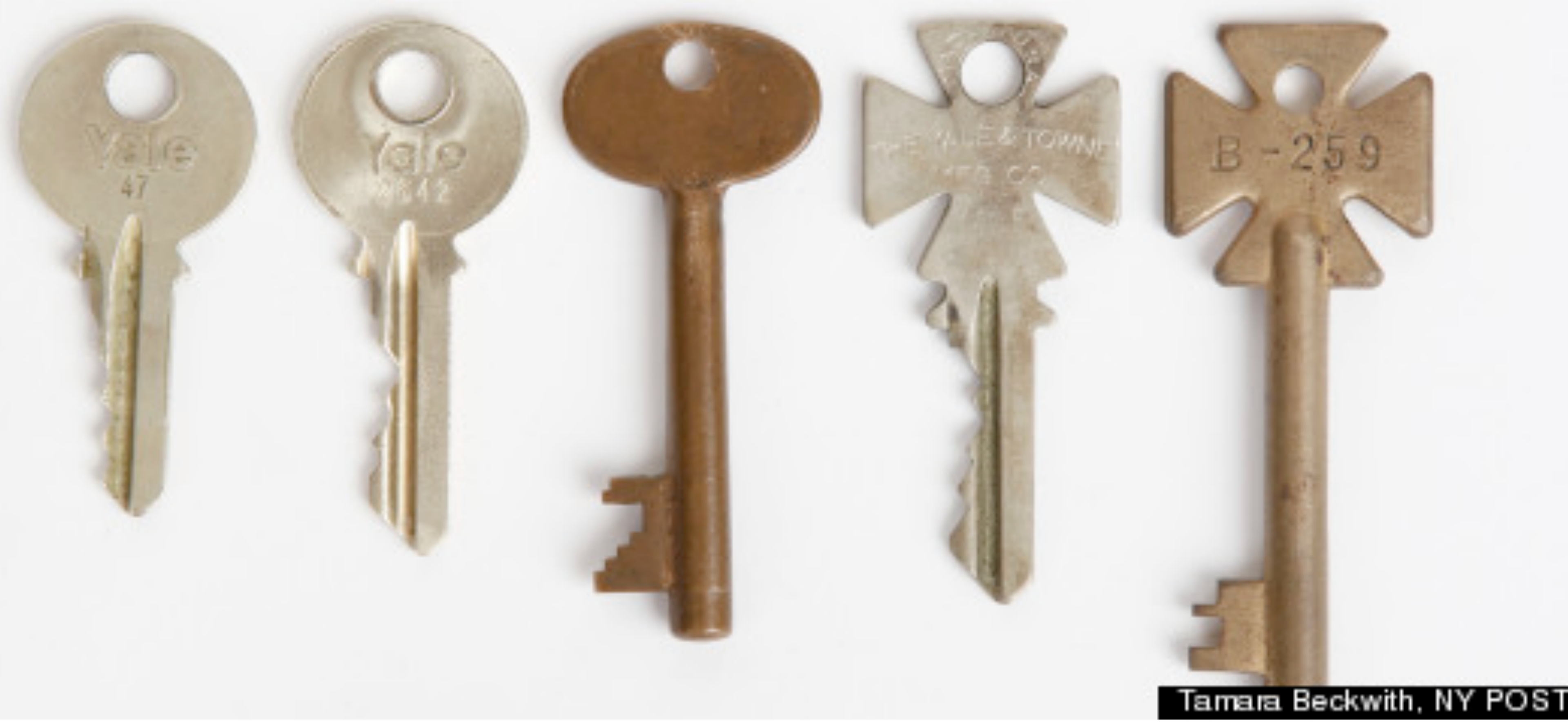
Schlage introduces a new standard for key control. Schlage's high-security Everest Primus and medium-security Everest cylinder and key management systems provide the optimal flexibility in key control and affordability. Our medium- and high-security products can be mixed in the same key system and are upgradable, enabling you to tailor security and cost to meet your exact needs. Both levels of security cylinders offer longer patent life (extends controlled key distribution), have keys that can be cut on standard machines (for maximum convenience and savings), and are available in a full range of cylinder types.

except on a 3d printer by MIT students David Lawrence and Eric van Albert in 2013…

$5 in nylon from Shapeways

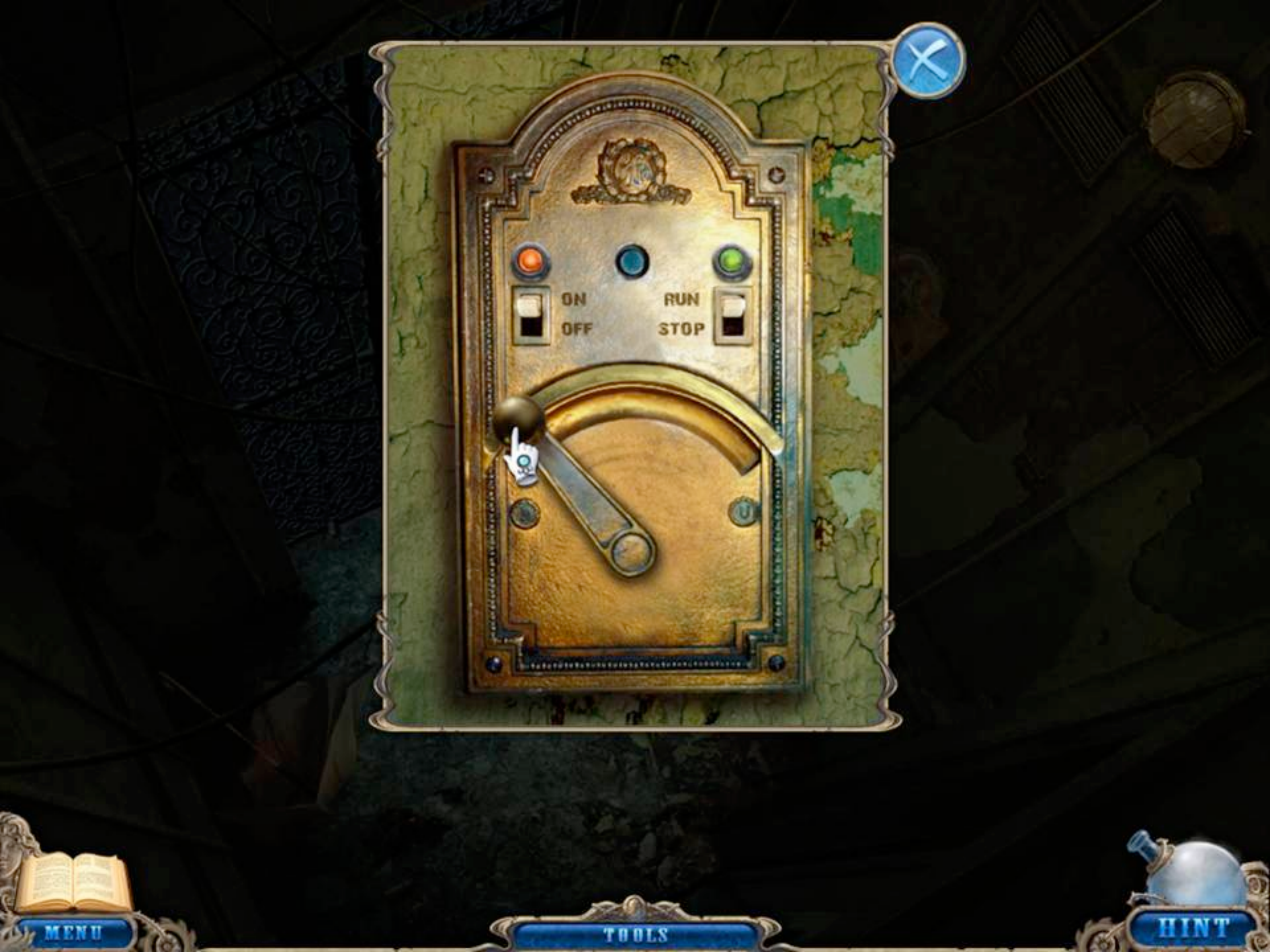
$150 in titanium from i.materialise

The Keys to the City… (sold on Ebay in 2012)

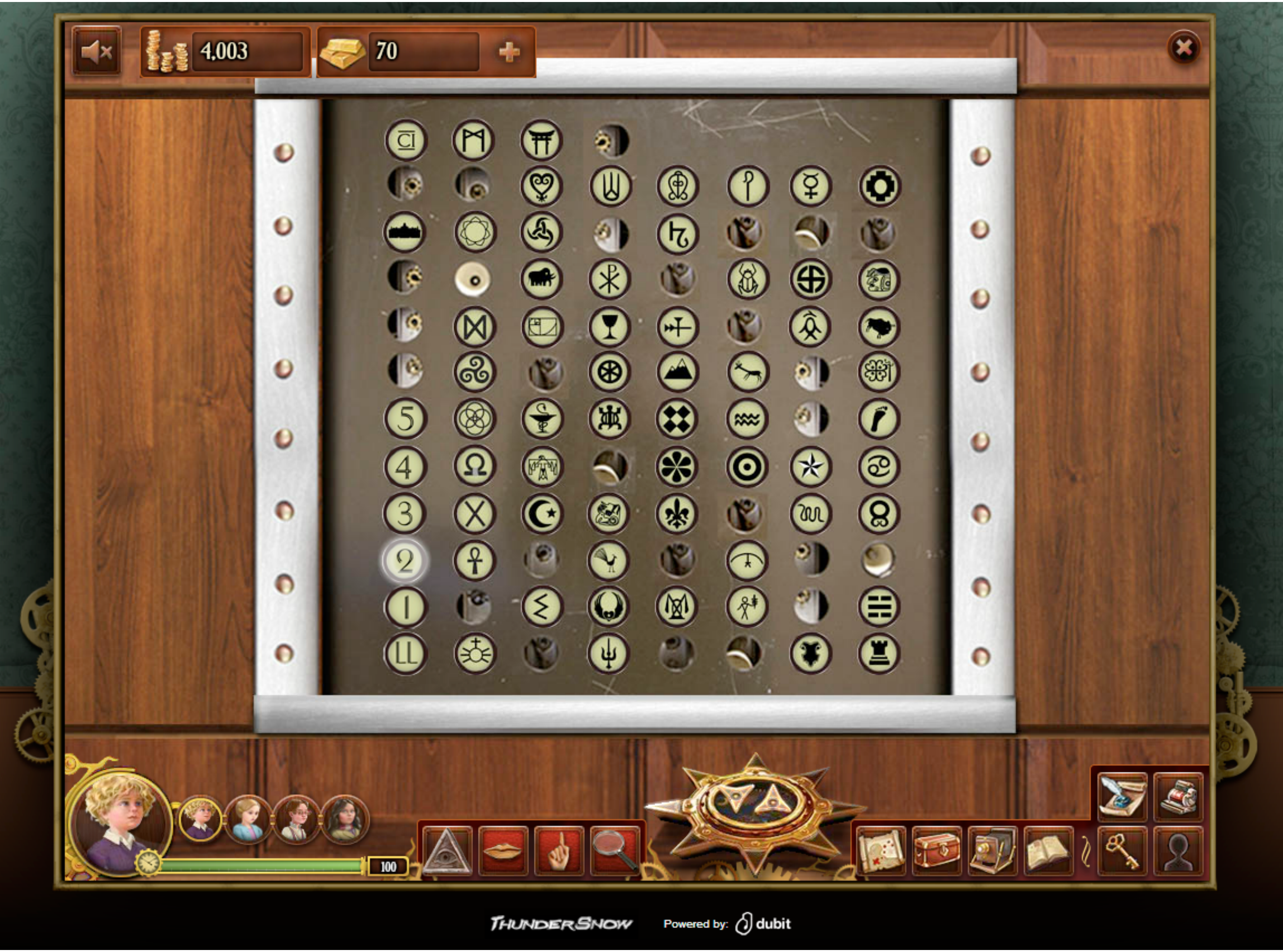


Tamara Beckwith, NY POST

elec panel elevator fire traffic light fire service fire alarm
box

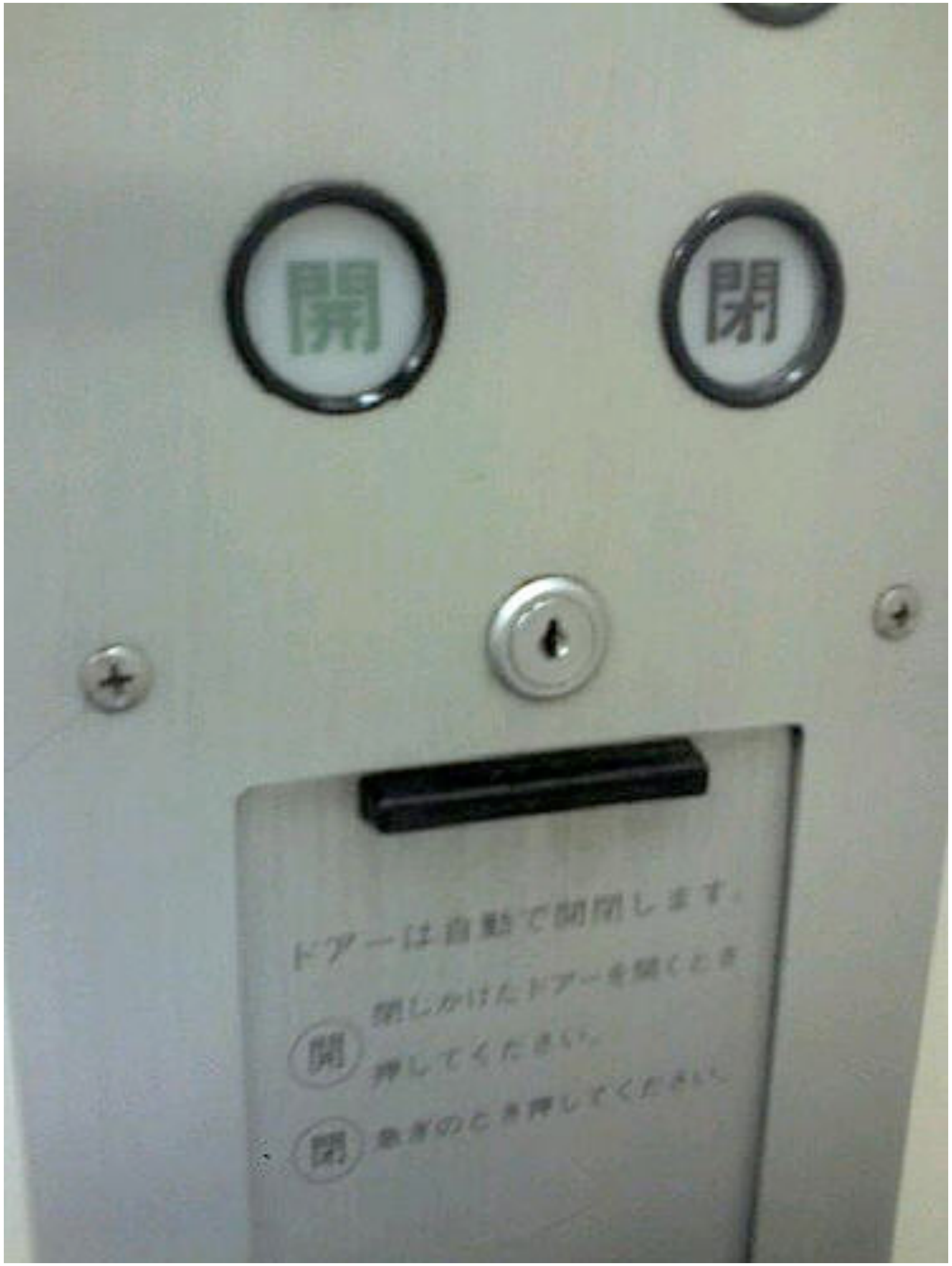

ON
OFF
RUN
STOP
MENU
TOOLS
HINT

VÉSZCSENGŐ
FJV
FŐVÁROSI FELVONÓJAVÍTÓ VÁLLALAT
BUDAPEST XIII. LEHEL ÚT 27-29
3
2
1/2


4,003
70
5
4
3
2
1
LL
100
THUNDERSNOW
Powered by: dubit

11
12
9
10
7
8

SAMSUNG
ROOM 501

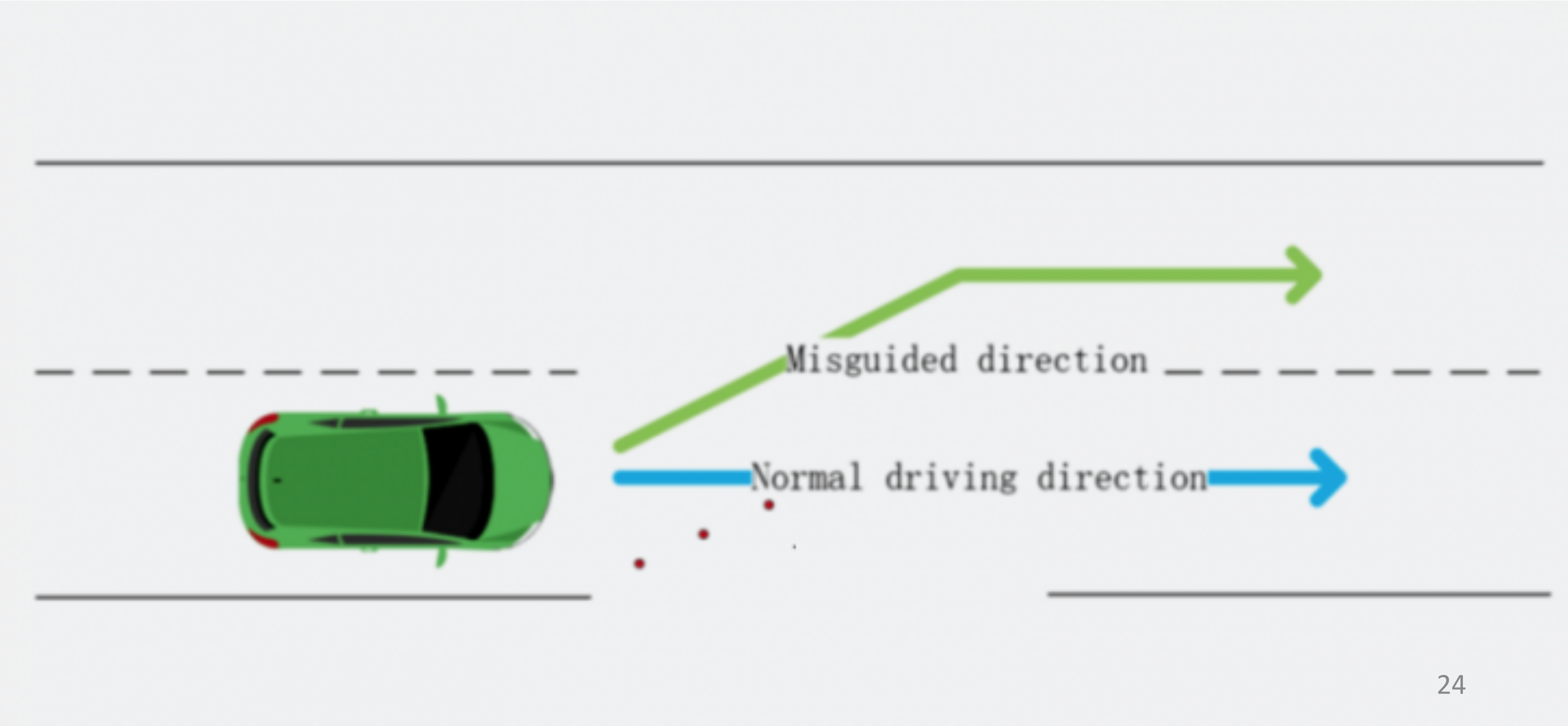

開
閉
ドアーは自動で開閉します。
閉じかけたドアーを開くとき
開 押してください。
閉 急ぎのとき押してください。

Lots of critical infrastructure is "keyed alike"

- Few things involving money, but everything operational (ATM safe versus upper housing).

Driving using sensors and image processing

- Trick Tesla into changing lanes by putting small circular stickers on the road (Tencent Keen Lab)

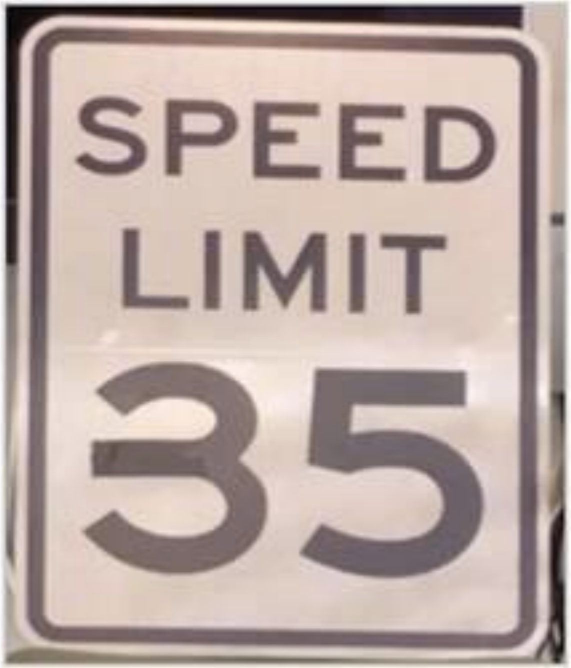


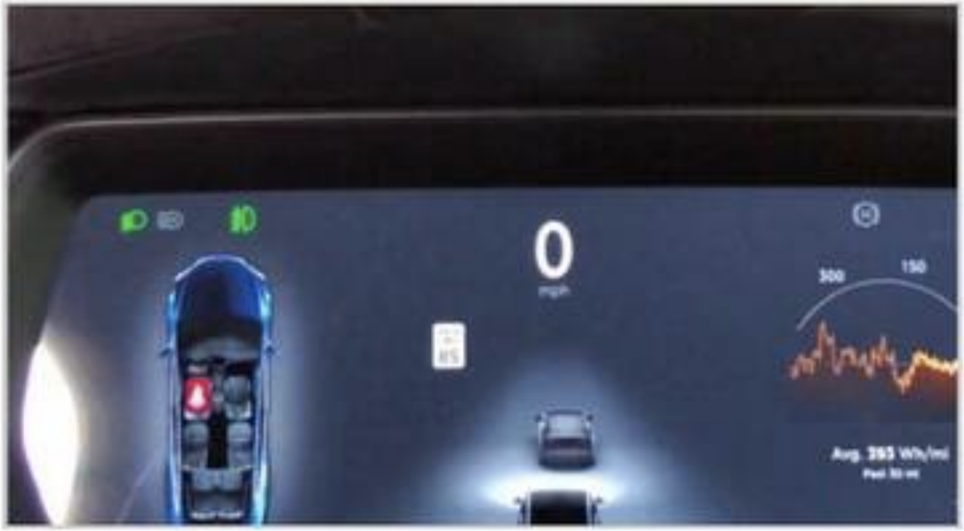
- Spoofing images of road signs on a digital billboard or pedestrians projected on the road for only a few frames (Yisroel Mirsky) https://youtu.be/-E0t_s6bT_4

Do airgapped networks still work? Not so much anymore.

- Many signals can be used (by installed malware) to covertly exfil data from a Secret network
- Link encryptor with flashing LED on the input port
- The Ben Gurion researchers are whizzes at this…
- Invisible changes in screen color/brightness: https://arxiv.org/pdf/2002.01078.pdf
- Modulating power lines, generating ultrasonic, hard drive, fan sound, heat exchange between computers, FM transmission using video card, RF on usb connector with no special hardware, etc.
- changing room temperature

Or with 3” of black tape



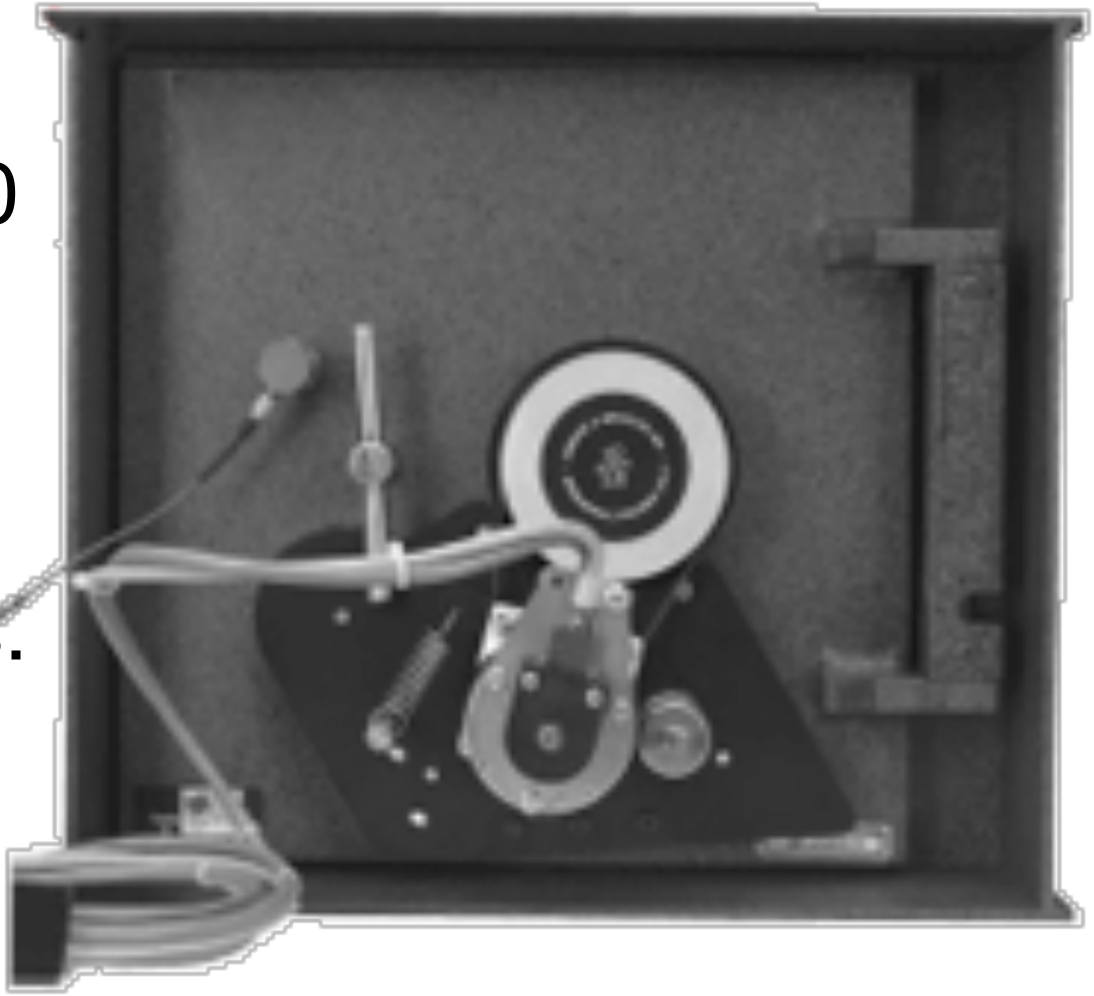


Softdrill (a PC peripheral)

Works on - S&G 6730, LaGard 3330 and Ilco 673.

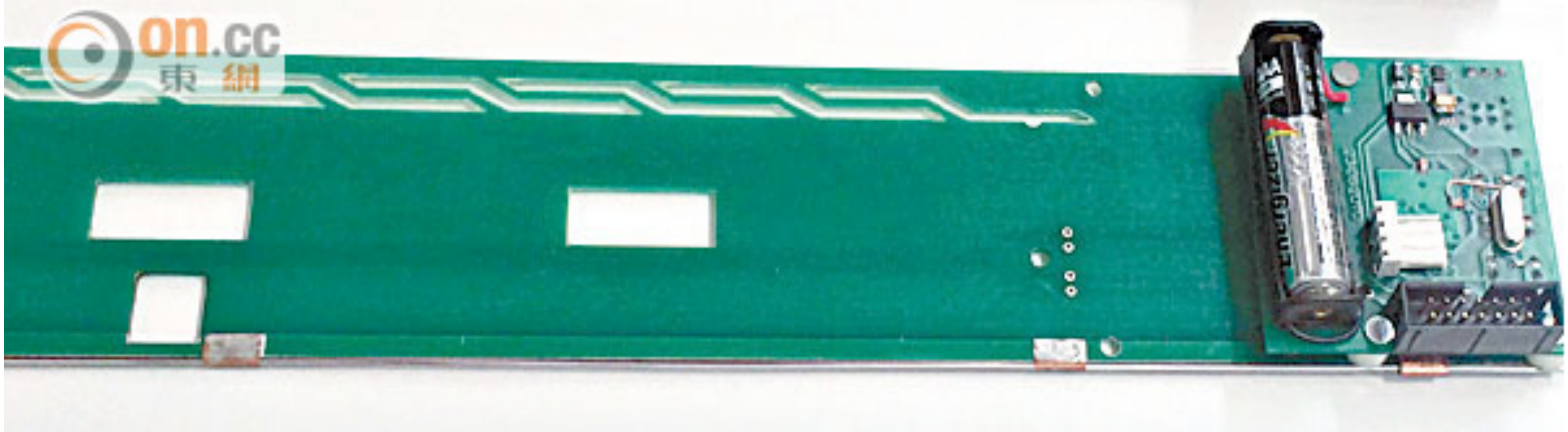
24 lb. $7k

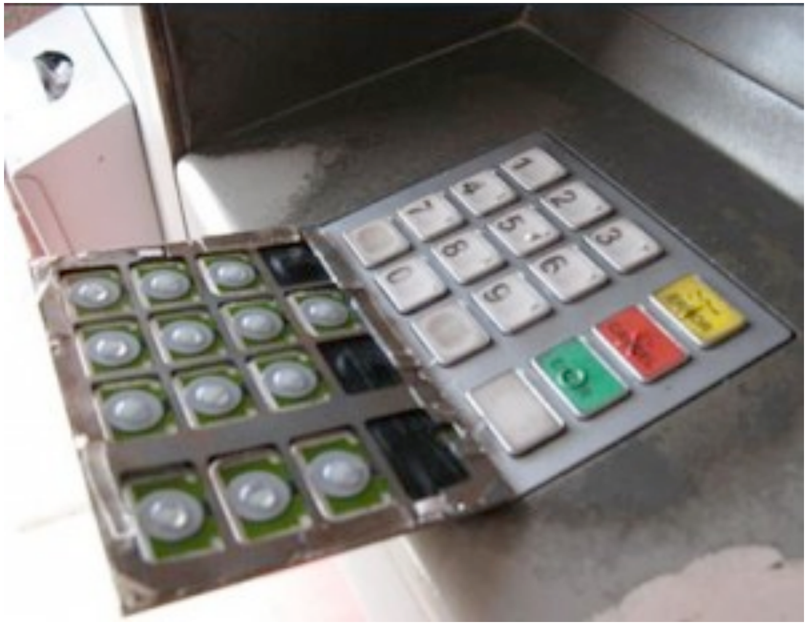
Average time to open: < 30 minutes.



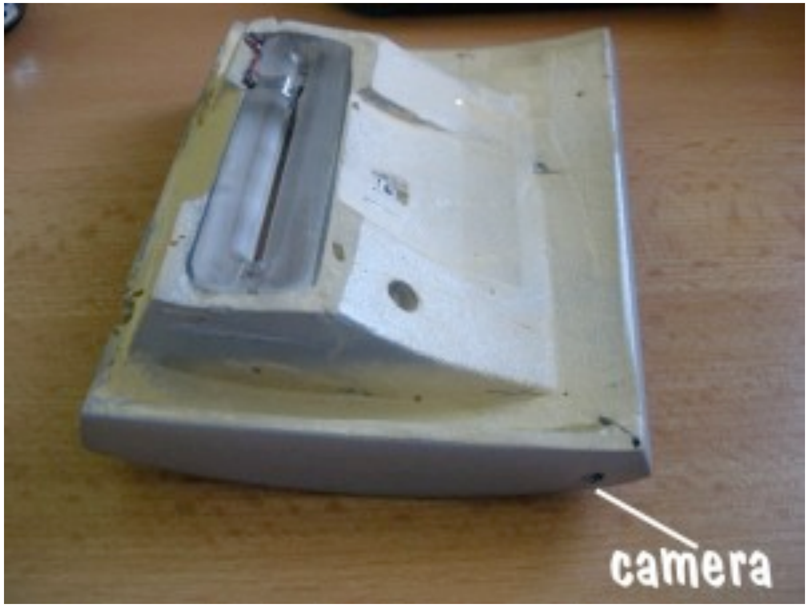
Divisão de Investigação de
Crimes Informáticos

新聞

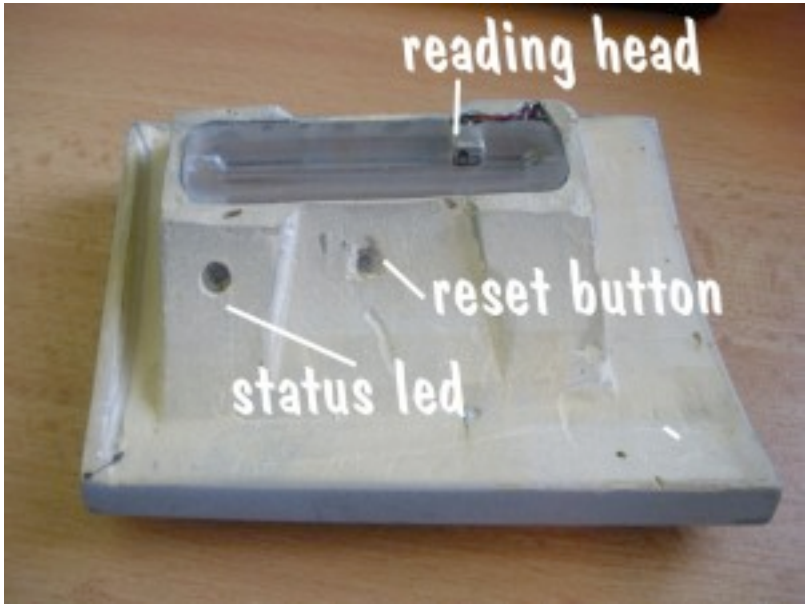



1
2
3
4
5
6
7
8
9
0

1
2
3
4
5
6
7
8
9
0

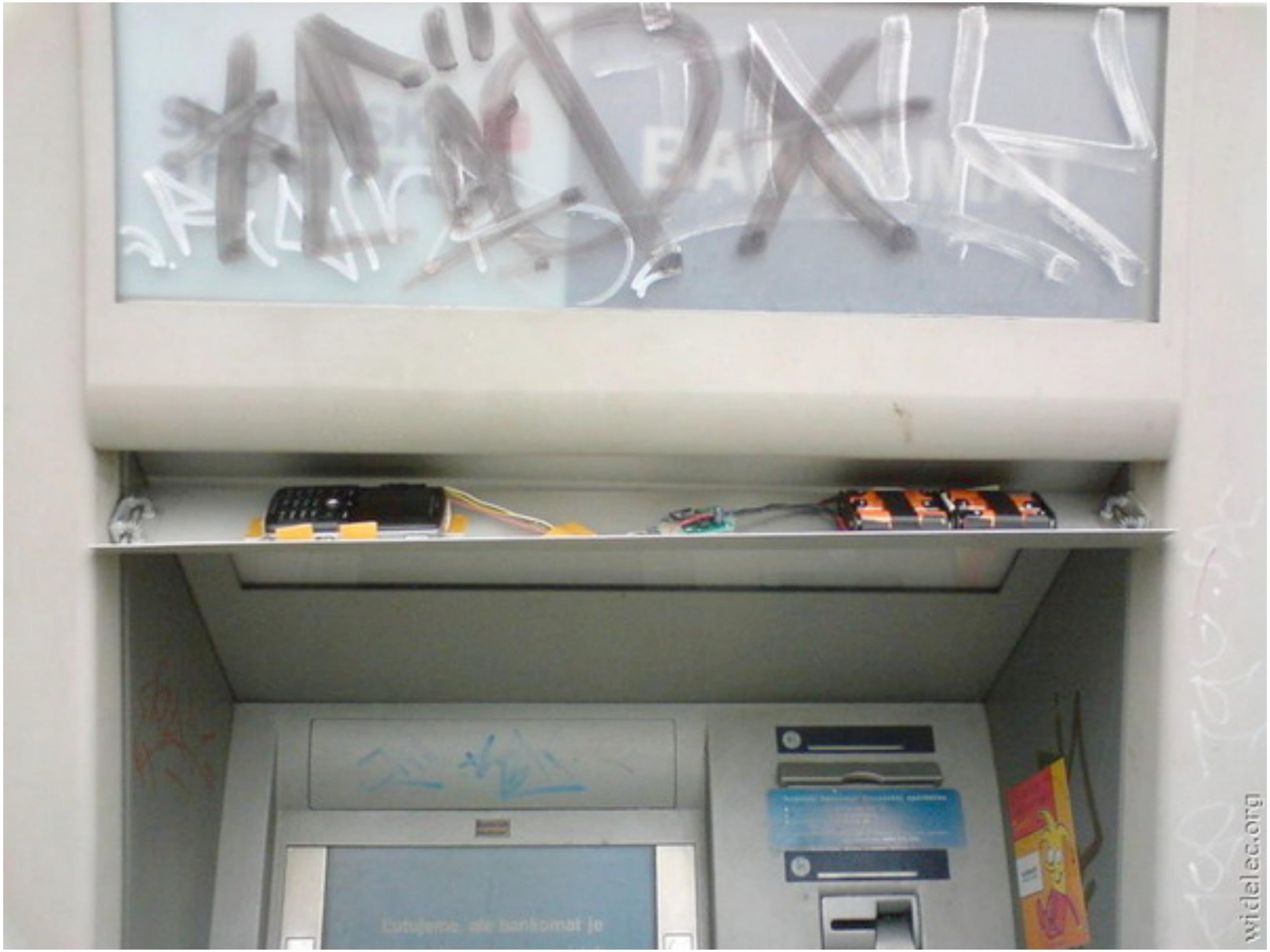


camera



reading head
reset button
status led

widelec.org



Litujeme, ale bankomat je
widelec.org

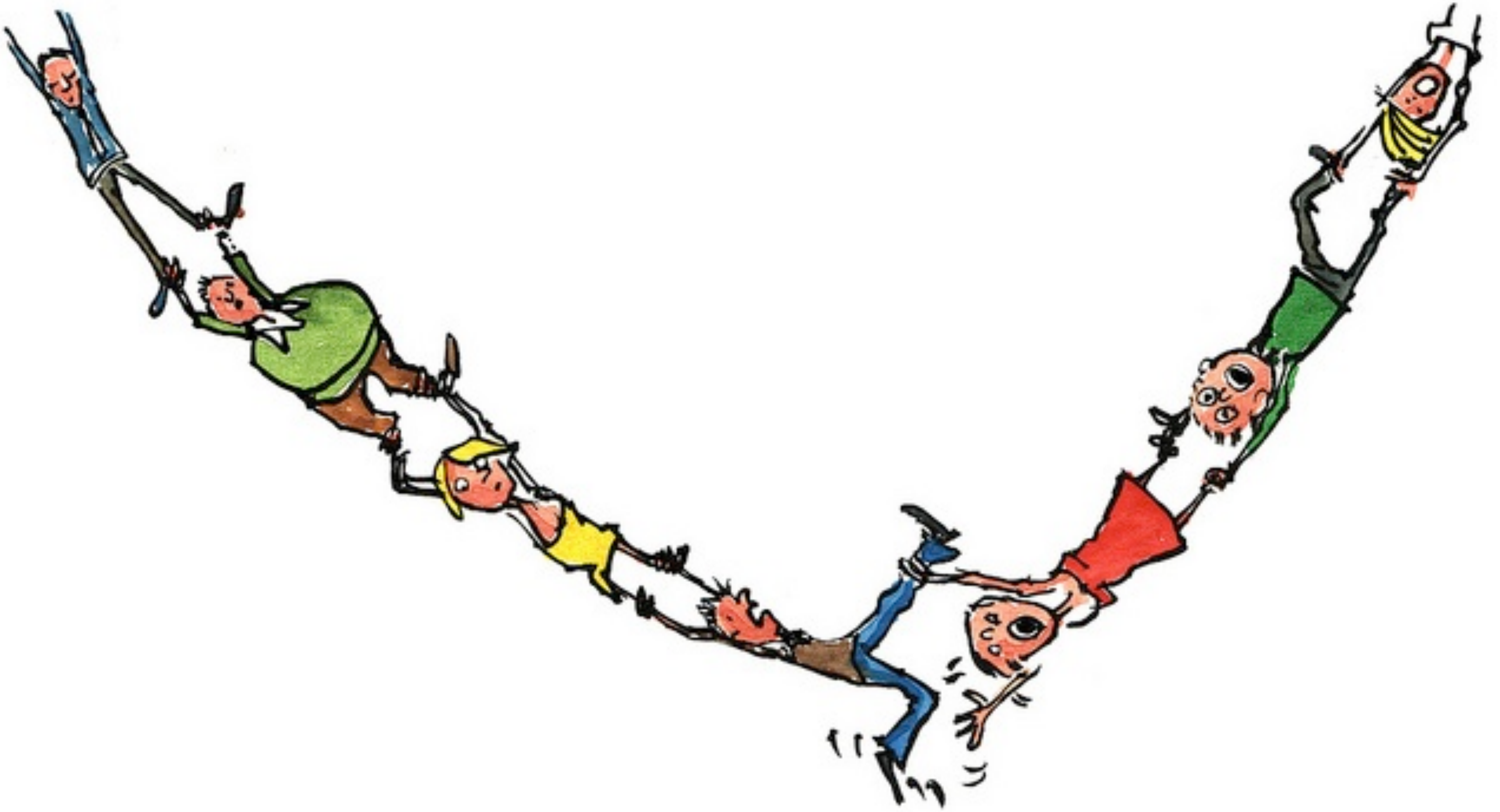
http://www.idealreceiver.com/gas-pump-skimmer.php

http://www.idealreceiver.com/diebold-atm-skimmer.php

http://www.idealreceiver.com/rfid-credit-card-skimmer.php

Bad guys will attack the weakest links.

… one of which is often a human link



Keystroke loggers aka keyloggers

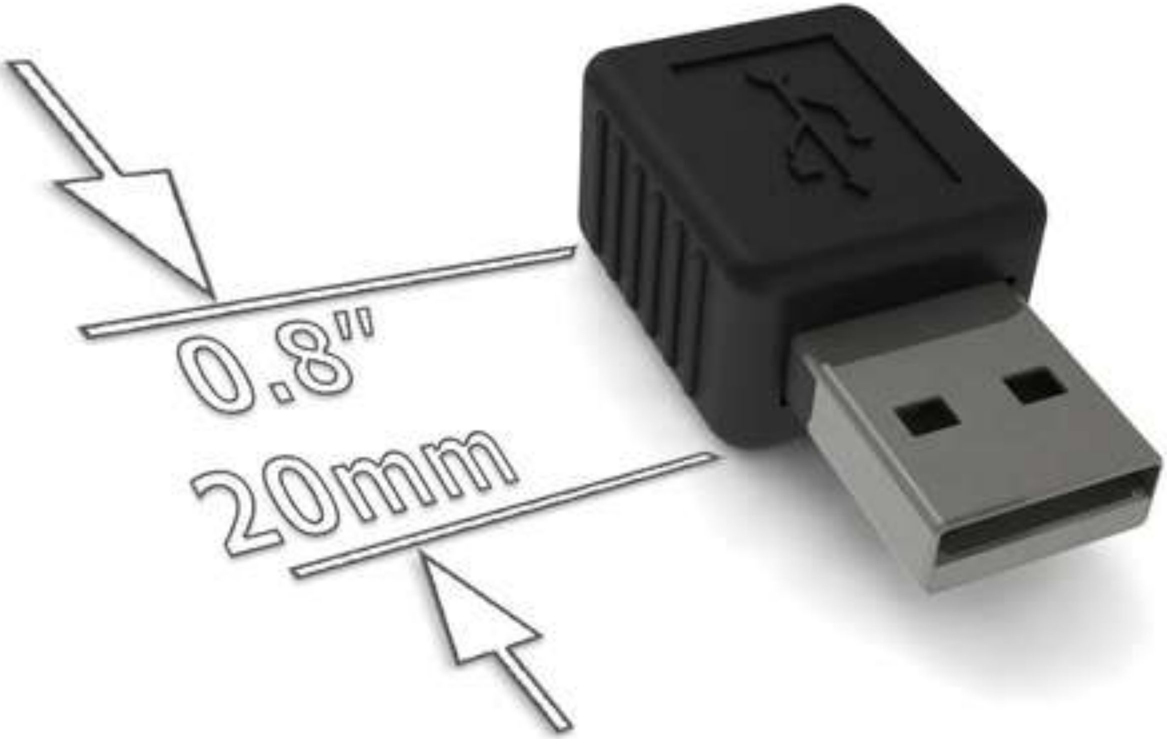
Old school:

For Microsoft wireless keyboards (Samy Kamkar, 2015)

https://samy.pl/keysweeper/

New school is much more stealthy:

https://www.keelog.com/keygrabber-pico/



(And surprisingly affordable…)

An external cable

or inside the keyboard

https://www.keelog.com/forensic-keylogger/

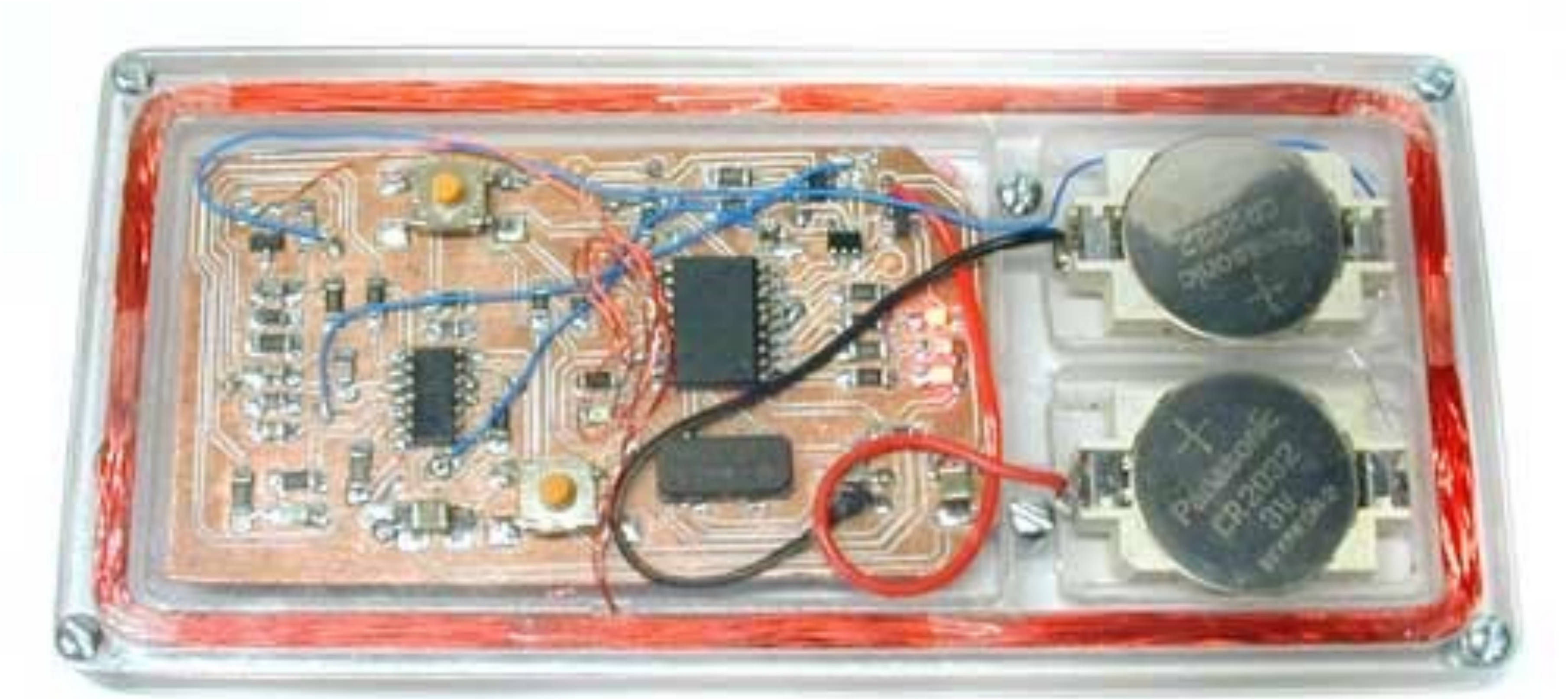
Consequences of cheap processing

- Acoustic emanations from keyboards can be used to detect passwords (and everything else).

Asonov and Agarwal, IBM Almaden, 2004

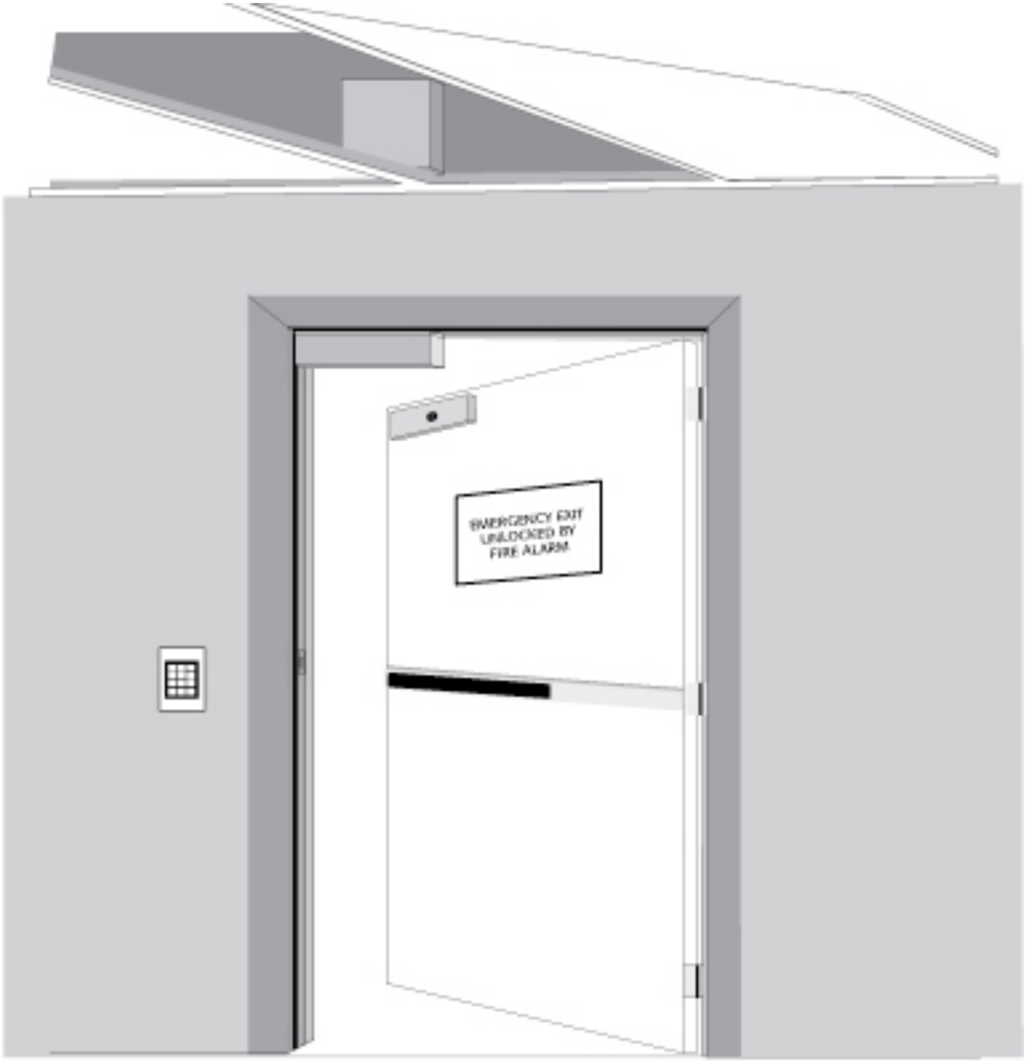
Zhuang, Zhou, Tygar, UC Berkeley, 2005

Prox card replay (200M simple prox cards out there) (Westhues, 2005)



https://archive.org/details/Recon2005_Jonathan_Westhues

A few random notes, if time allows:


EMERGENCY EXIT
UNLOCKED BY
FIRE ALARM

Detective controls and agile response are more effective than preventive controls

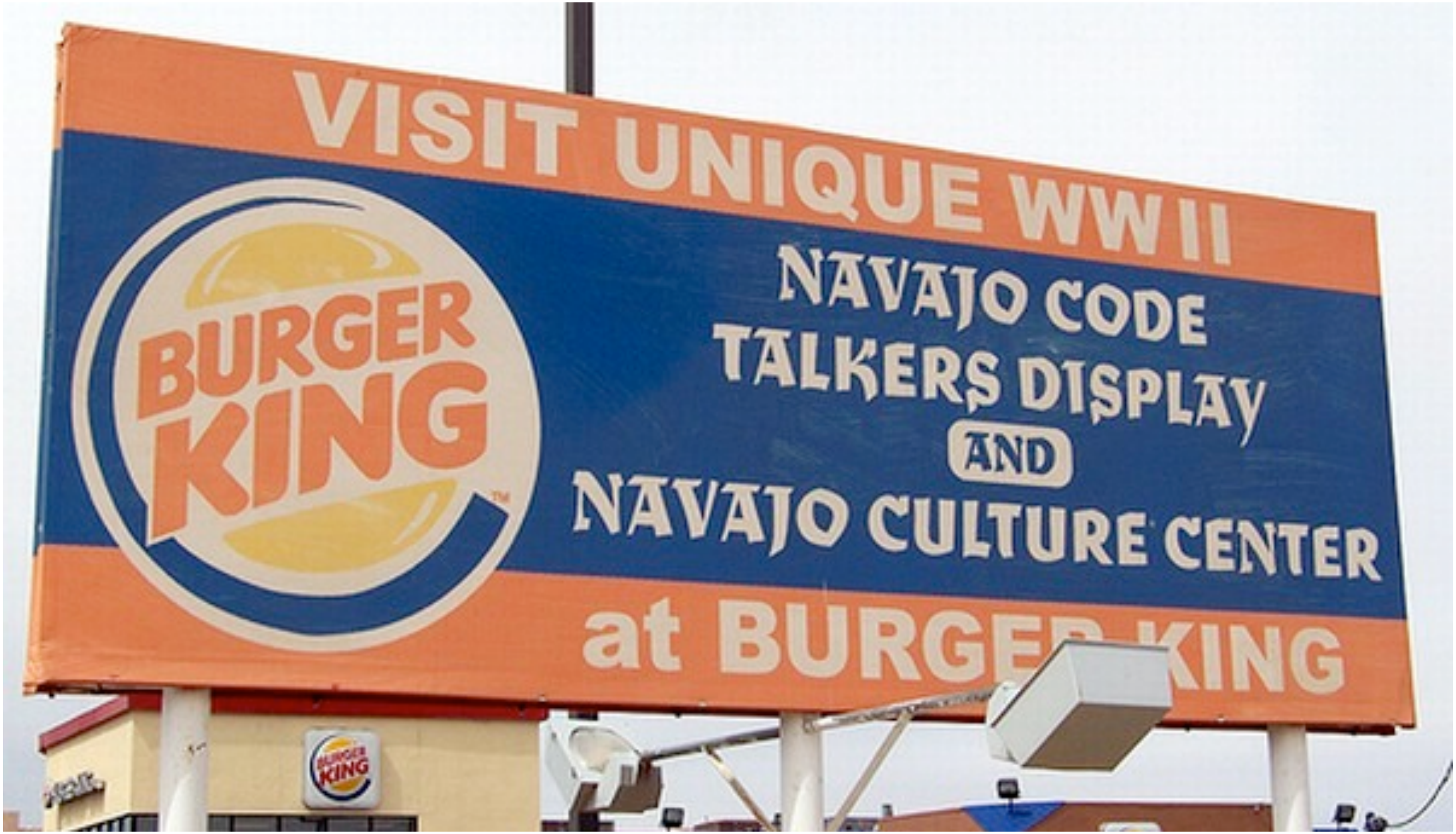
- Which is why we use alarm systems and CCTV.
- Even the highest quality safes are only rated for 60 minutes with tools, burn bars/torches, nitroglycerin

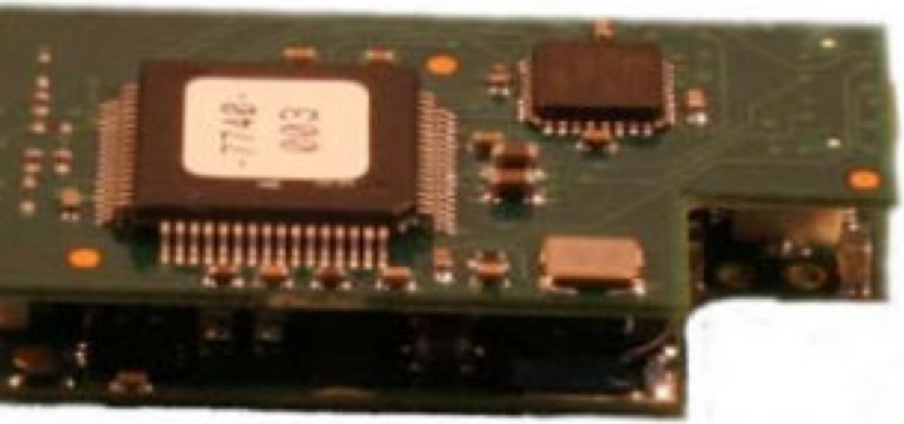
(insure up to $5M)

Security through obscurity has some value

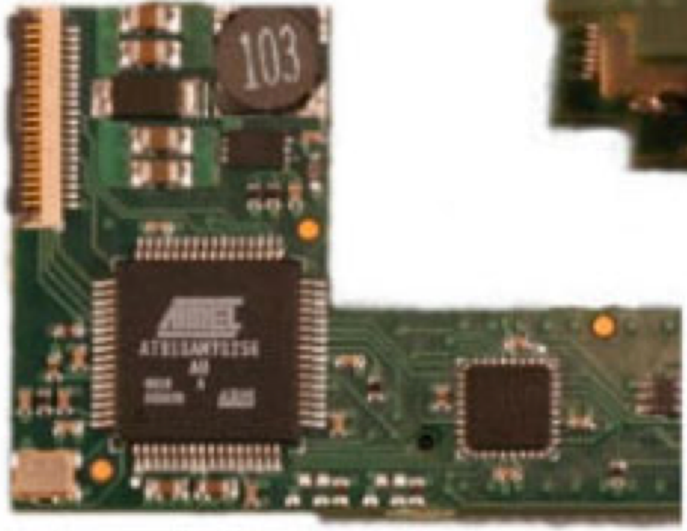
Navajo Code Talkers at Iwo Jima in 1943

And today


VISIT UNIQUE WW II
NAVAJO CODE
TALKERS DISPLAY
AND
NAVAJO CULTURE CENTER
at BURGER KING
BURGER KING



(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 2950



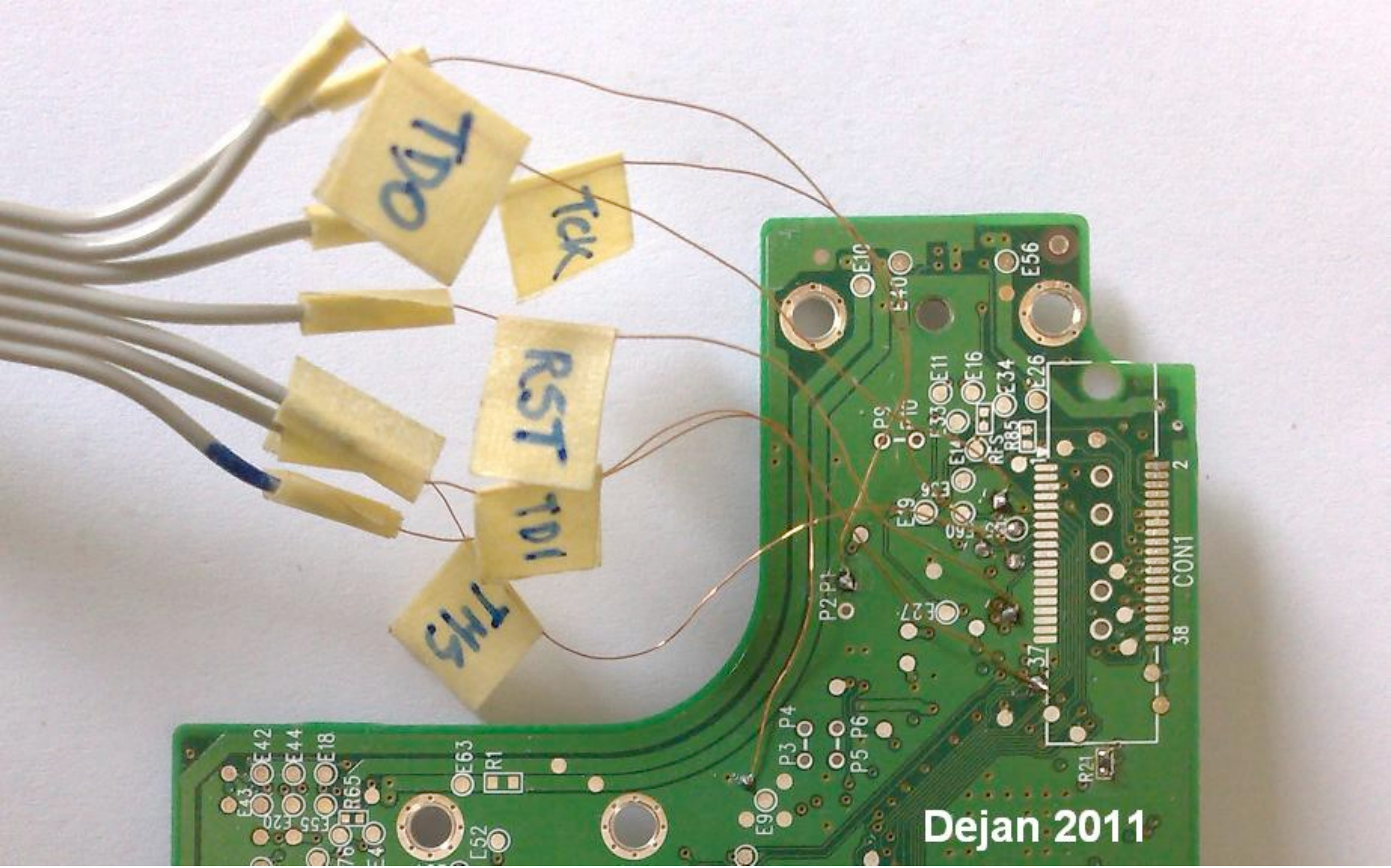
(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950

ANGRYMONK: Inserts itself into the firmware of hard drives made by Western Digital, Seagate, Maxtor and Samsung.

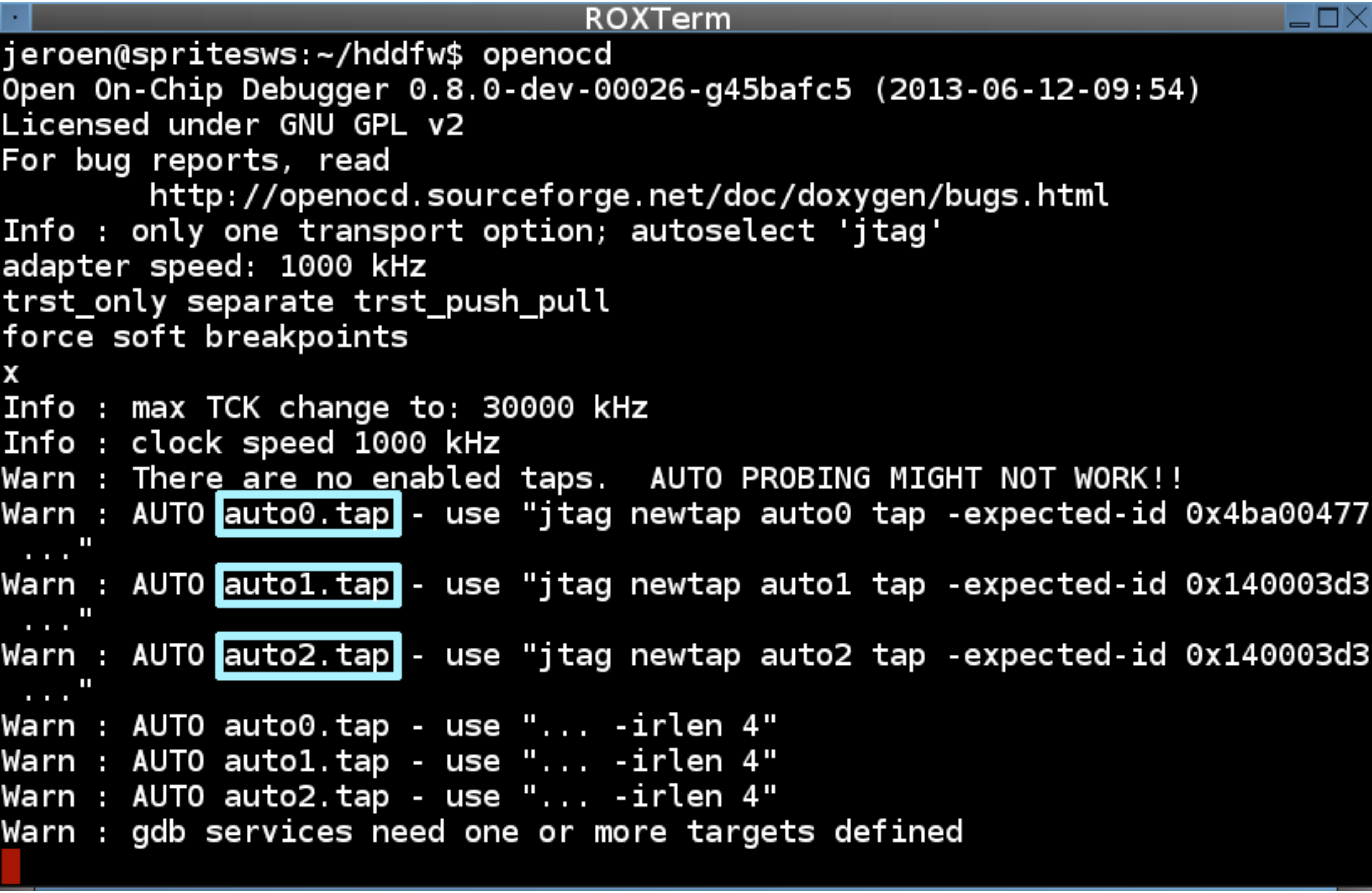
Zaddach, J., Kurmus, A. et al: “Implementation and implications of a stealth hard-drive backdoor” - ACSAC 2013

This paper analyzes the catastrophic loss of security that occurs when hard disks are not trustworthy. First, we show that it is possible to compromise the firmware of a commercial off-the-shelf hard drive, by resorting only to public information and reverse engineering. Using such a compromised firmware, we present a stealth rootkit that replaces arbitrary blocks from the disk while they are written, providing a data replacement back-door. The measured performance overhead of the compromised disk drive is less than 1% compared with a normal, non-malicious disk drive. We then demonstrate that a remote attacker can even establish a communication channel with a compromised disk to infiltrate commands and to ex-filtrate data. In our example, this channel is established over the Internet to an unmodified web server that relies on the compromised drive for its storage, passing through the original webserver, database server, database storage engine, filesystem driver, and block device driver. Additional experiments, performed in an emulated disk-drive environment, could automatically extract sensitive data such as /etc/shadow (or a secret key file) in less than a minute. This paper claims that the difficulty of implementing such an attack is not limited to the area of government cyber-warfare; rather, it is well within the reach of moderately funded criminals, botnet herders and academic researchers.

See spritemods.com for some clever hard drive reverse engineering…



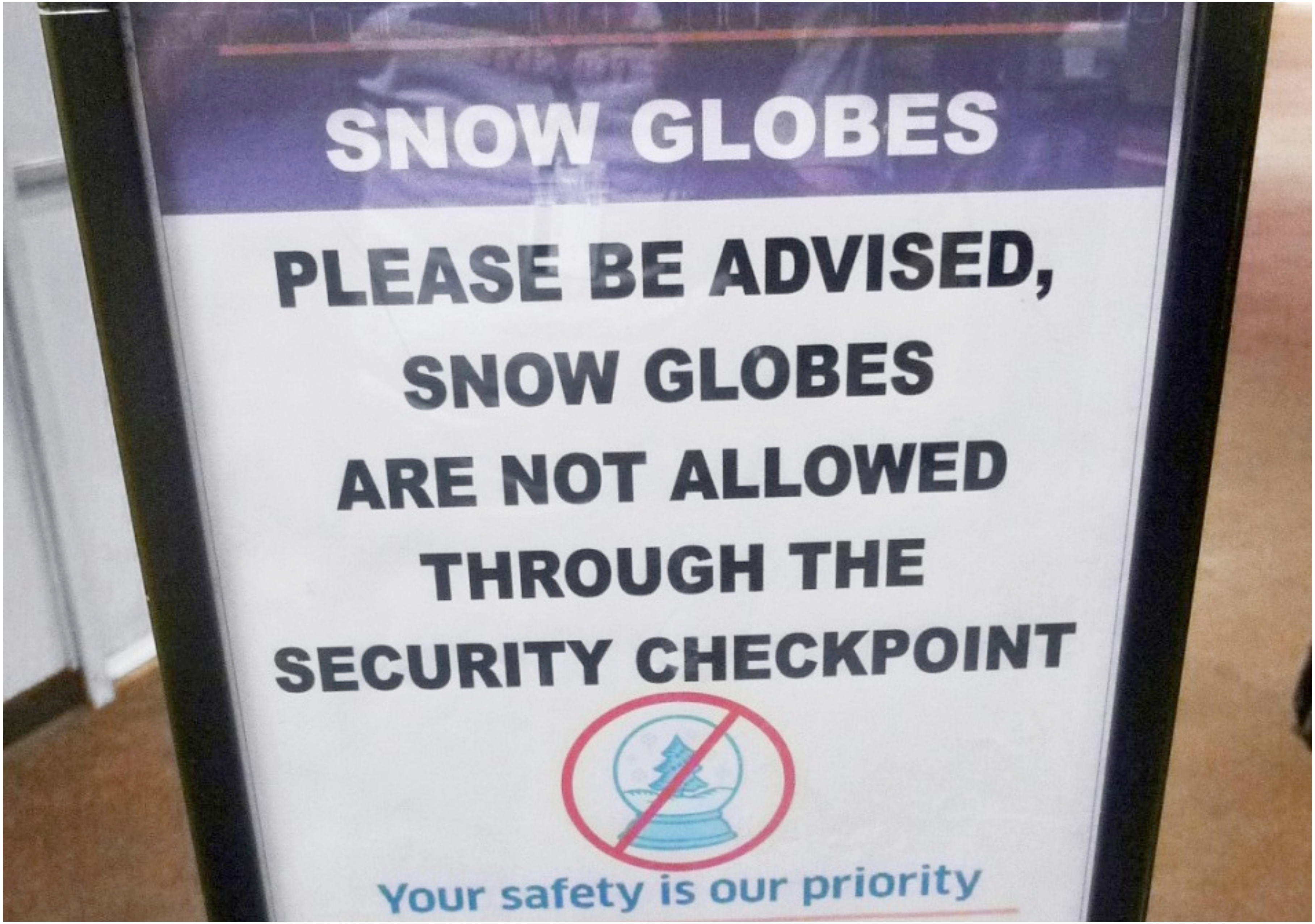
http://forum.hddguru.com/viewtopic.php?t=20324



```
jeroen@spritesws:~/hddfw$ openocd
Open On-Chip Debugger 0.8.0-dev-00026-g45bafc5 (2013-06-12-09:54)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.sourceforge.net/doc/doxygen/bugs.html
Info : only one transport option; autoselect 'jtag'
adapter speed: 1000 kHz
trst_only separate trst_push_pull
force soft breakpoints
x
Info : max TCK change to: 30000 kHz
Info : clock speed 1000 kHz
Warn : There are no enabled taps.  AUTO PROBING MIGHT NOT WORK!!
Warn : AUTO auto0.tap - use "jtag newtap auto0 tap -expected-id 0x4ba00477
 ..."
Warn : AUTO auto1.tap - use "jtag newtap auto1 tap -expected-id 0x140003d3
 ..."
Warn : AUTO auto2.tap - use "jtag newtap auto2 tap -expected-id 0x140003d3
 ..."
Warn : AUTO auto0.tap - use "... -irlen 4"
Warn : AUTO auto1.tap - use "... -irlen 4"
Warn : AUTO auto2.tap - use "... -irlen 4"
Warn : gdb services need one or more targets defined
```

The world keeps changing

{Smaller, faster, cheaper, less wired, always on} {computer, storage, sensors} implies you MUST reexamine assumptions, design and implementation choices made {10, 5, even 2} years ago -- attacks that were impractical then may be practical now.



SNOW GLOBES

PLEASE BE ADVISED,
SNOW GLOBES
ARE NOT ALLOWED
THROUGH THE
SECURITY CHECKPOINT

Your safety is our priority

More questions, please?