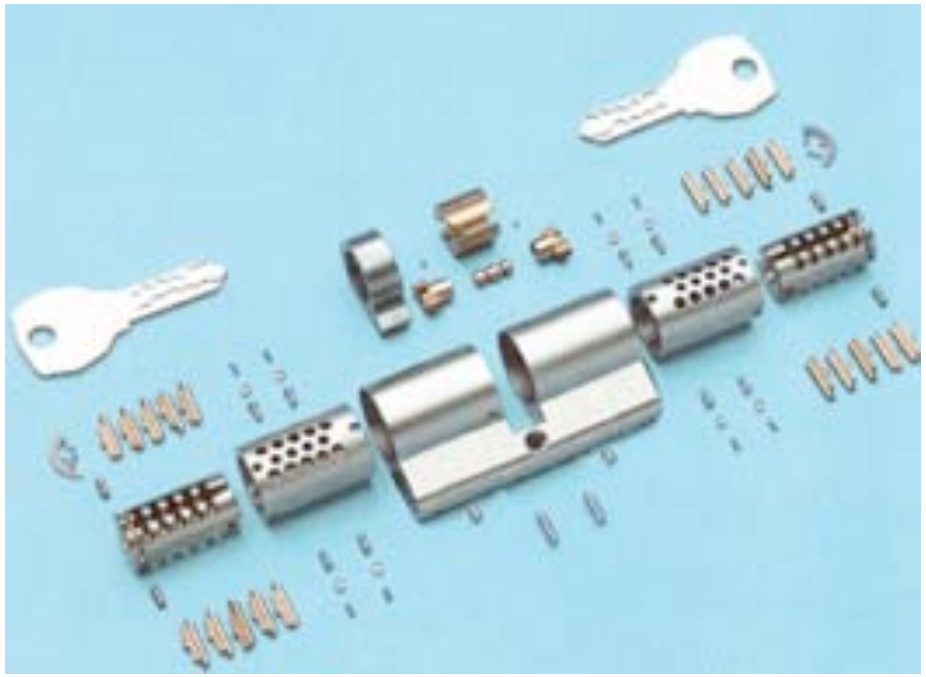
Lockpicking and IT Security

Walter Belgers, M.Sc, CISSP, CISA

TLP:WHITE

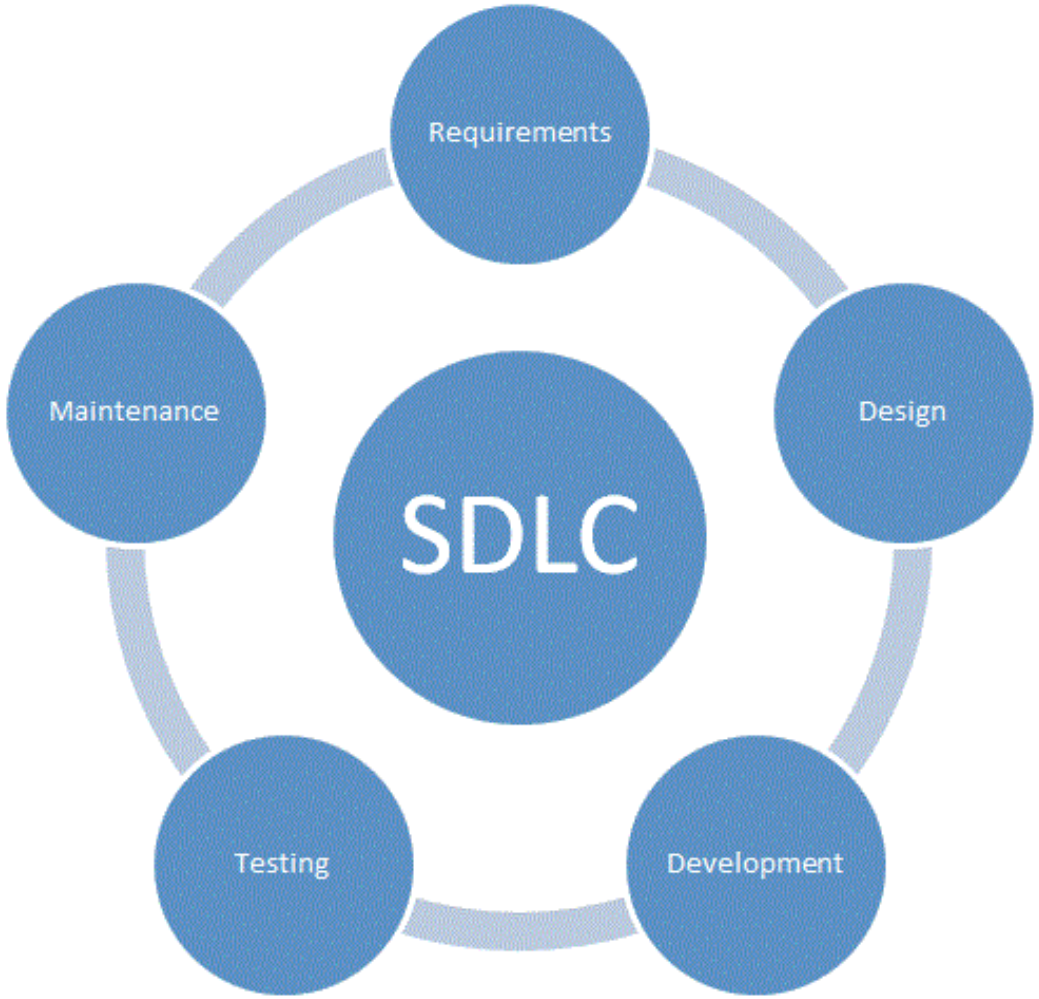

PROPF
GANDA
TOOL
The Open Organisation Of Lockpickers
NDHOVEN

- 20 years of lockpicking experience
- President of TOOOL, The Open Organisation of Lockpickers
- Fastest Dutch lockpicker ;-)




PATENT
B66


OWNED!
by spk


Requirements
Design
Development
Testing
Maintenance
SDLC

Design - software

- Security often a small component in software and hence, often an afterthought
- Functionality is more important than security


esa
ariane
esa

Design - locks

- Locks are always there to provide security, so no afterthought
- Lock manufacturers are good in specifying requirements
- Risks are pretty well understood (but not by all!)
- Locks are tested (e.g. for certification)

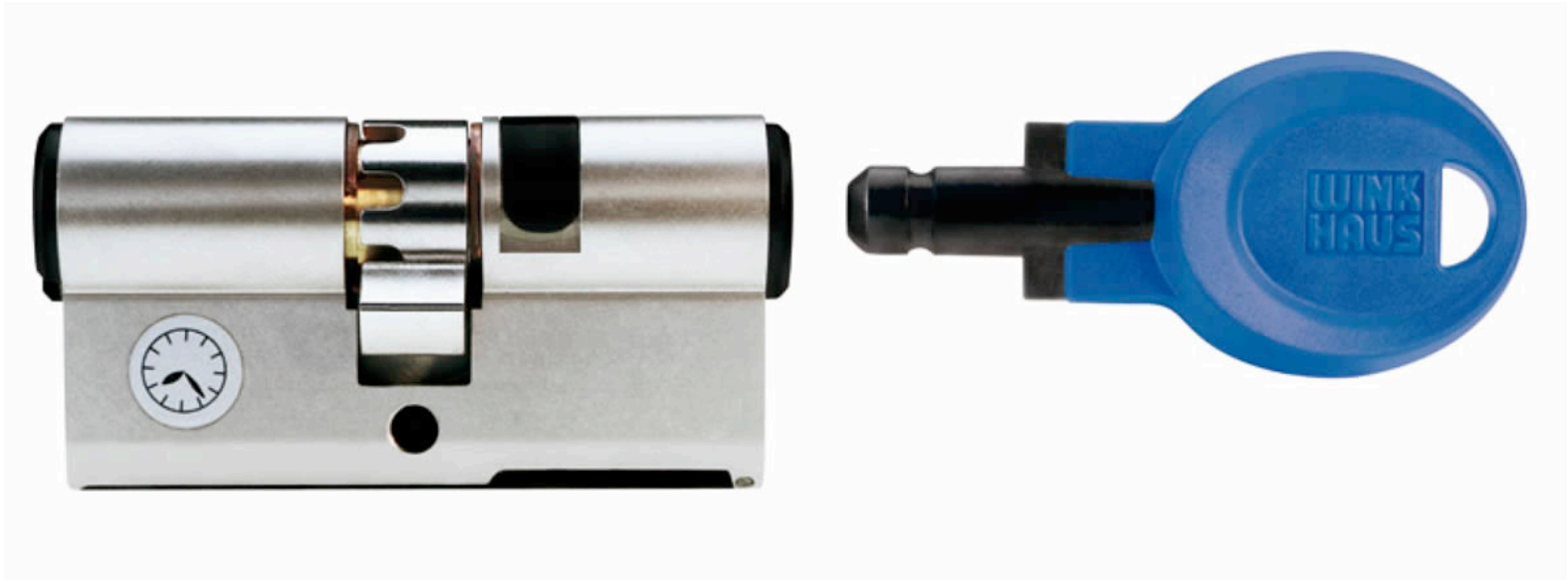
Design - locks

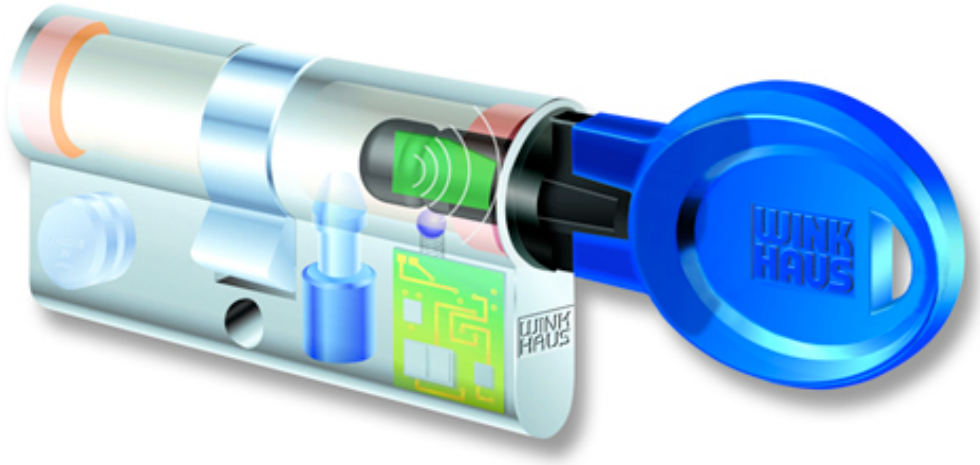
- Secure against what?
  - Key control (who can copy)
  - Protection against destructive attacks (drilling, pulling, breaking)
  - Protection against non-destructive attacks (lockpicking, pickgun, bumping, impressioning)
  - Tight cost and space constraints

Design: KABA E-plex 5800

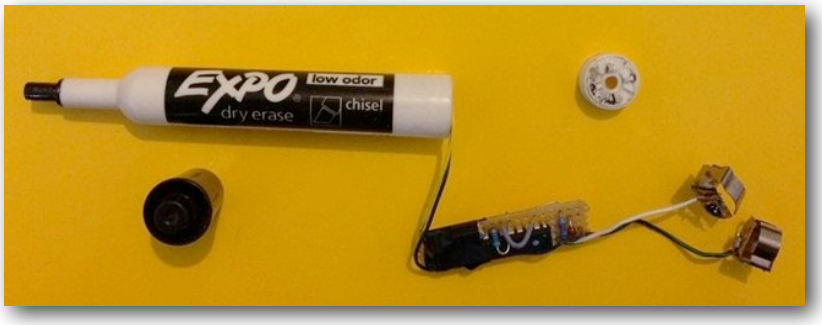
Defcon Lockpickers Open Card-And-Code Government Locks In Seconds

forbes.com


WINKHAUS

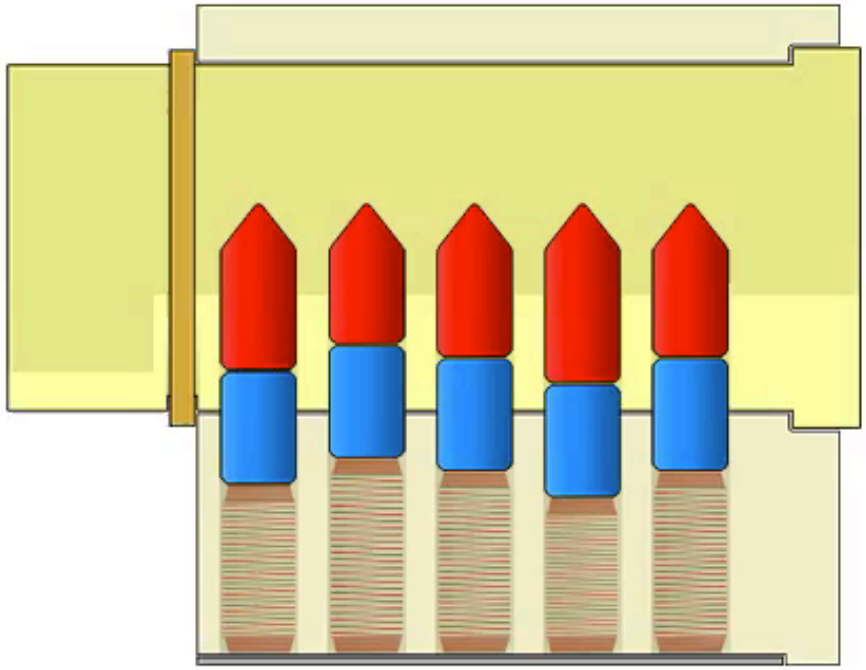

WINKHAUS
WINKHAUS

http://null-byte.wonderhowto.com/how-to/turn-innocent-dry-erase-marker-into-hotel-hacking-machine-0139534/



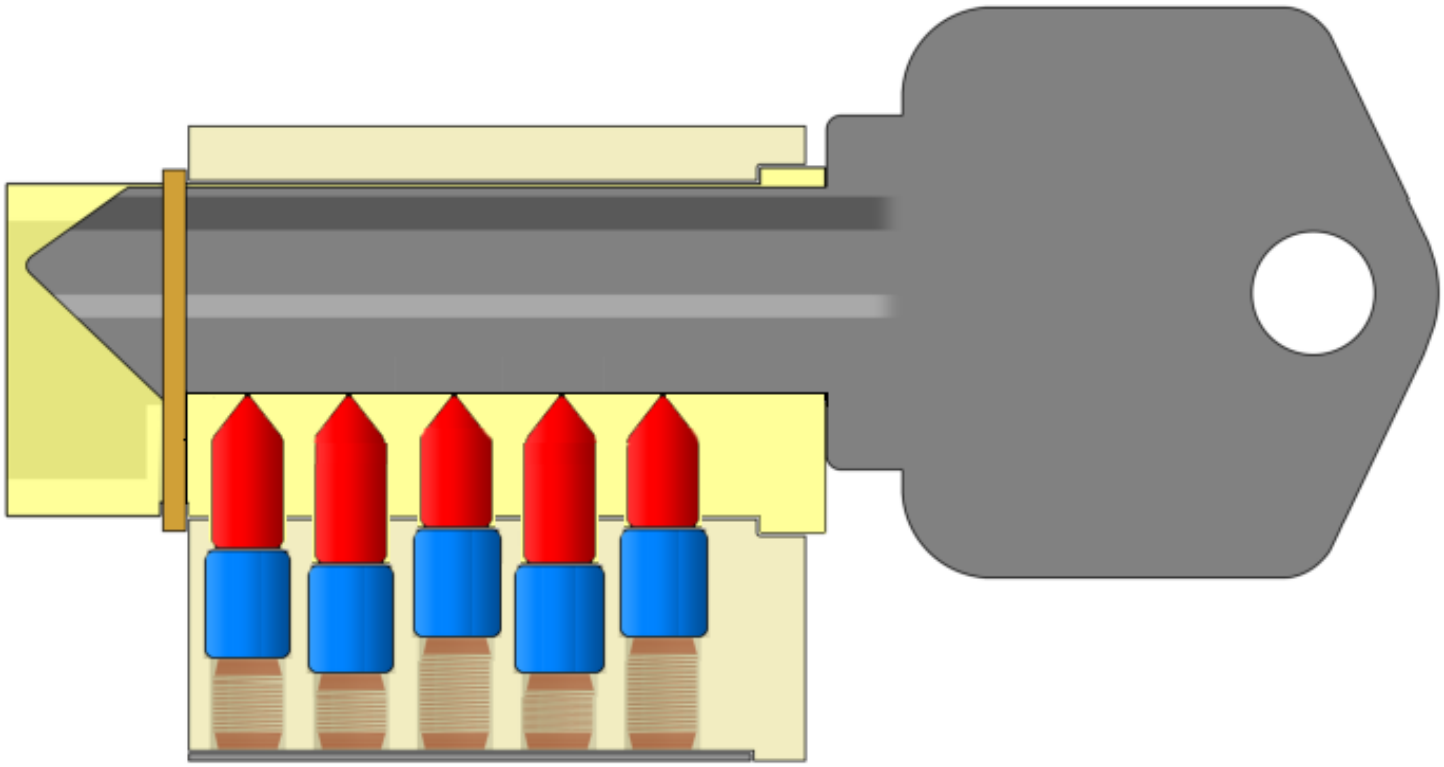
https://www.youtube.com/watch?v=6txFFS1TwSE

Implementation error



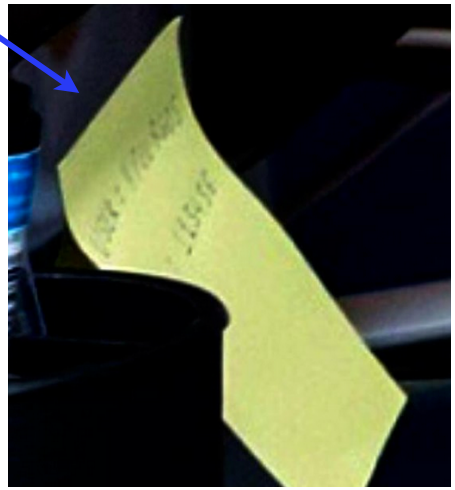
animation: Deviant Ollam

Implementation error



- Awareness is always a problem
  - Password guessing
  - Social Engineering

- Showing your keys..



Showing (master) keys

http://www.nbcbayarea.com/investigations/One-Gas-Pump-Key-Lets-Thieves-Steal-Your-ID-177999751.html

Showing (master) keys

ELECTRICAL PANEL KEY
- **What it does:** Opens street-lamp boxes and circuit-breaker panels in virtually every building in NYC
- **What you could do:** Shut off power to City Hall or a police station house
- **Who has it:** City electricians and contractors

FIRE ELEVATOR KEY
- **What it does:** Controls almost any elevator in the city. Unlocks fire-alarm panels in buildings
- **What you could do:** Send all the elevators in the Empire State Building to the ground floor, trapping everyone inside
- **Who has it:** FDNY and fire-safety workers

TRAFFIC LIGHT KEY
- **What it does:** Works on older versions of traffic-light control panels
- **What you could do:** Cause amassive traffic jam to tie up police/fire response
- **Who has it:** Transportation workers

FIREMAN SERVICE KEY "1620"
- **What it does:** Controls elevators and opens locked subway entrances, construction-site master key boxes and some firehouse doors
- **What you could do:** Take over the subways or One World Trade Center
- **Who has it:** FDNY and building engineers

FIRE ALARM BOX KEY
- **What it does:** Works on street alarm boxes
- **What you could do:** Set off alarm chaos

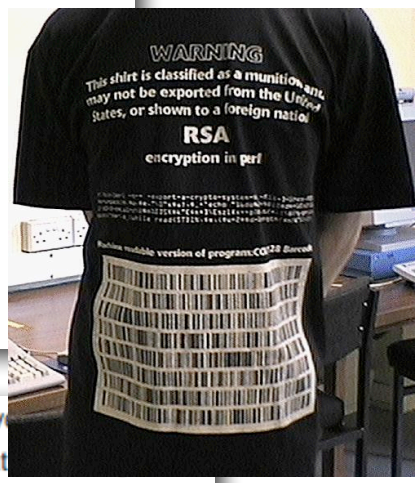

HUMAN

Backdoors

N.S.A. Able to Foil Basic Safeguards of Privacy on Web

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE
Published: September 5, 2013

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.



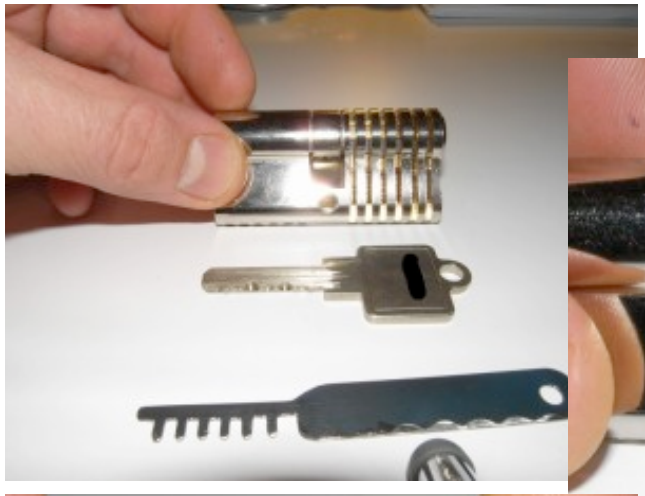
But on Nov. 5, 2003, Larry McVoy **noticed** that there was a code change in the CVS copy that did not hav record of approval. Investigation showed that the change had never been approved and, stranger yet, that not appear in the primary BitKeeper repository at all. Further investigation determined that someone had apparently broken in (electronically) to the CVS server and inserted this change.

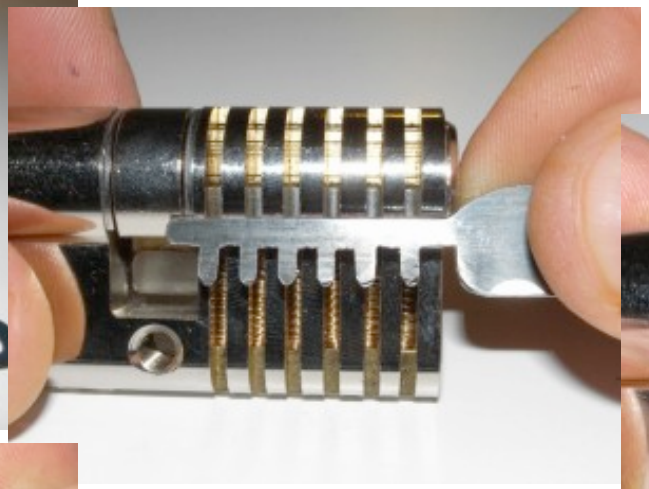
What did the change do? This is where it gets really interesting. The change modified the code of a Linux function called wait4, which a program could use to wait for something to happen. Specifically, it added these two lines of code:

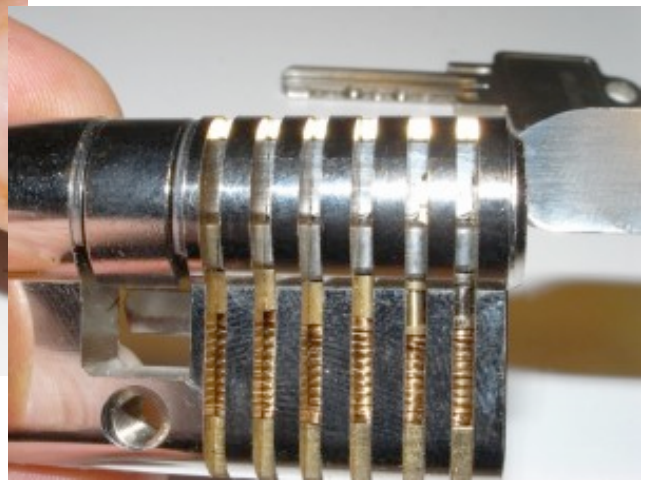
```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```

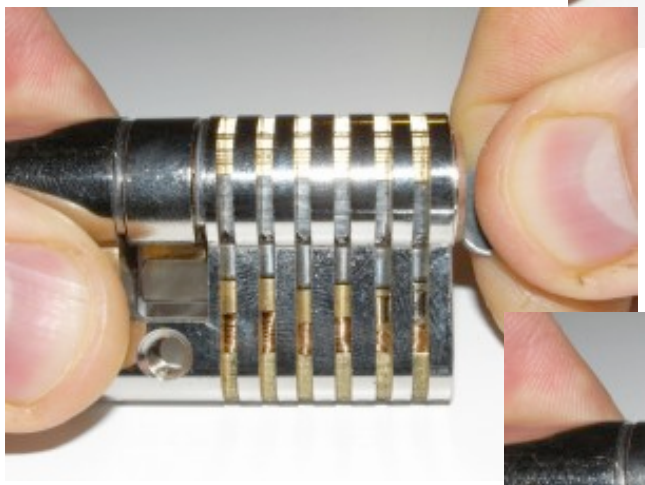

1
2
3
4
5
6
7
8
9
C
0
E
KEYWAYS
HOMESAFE

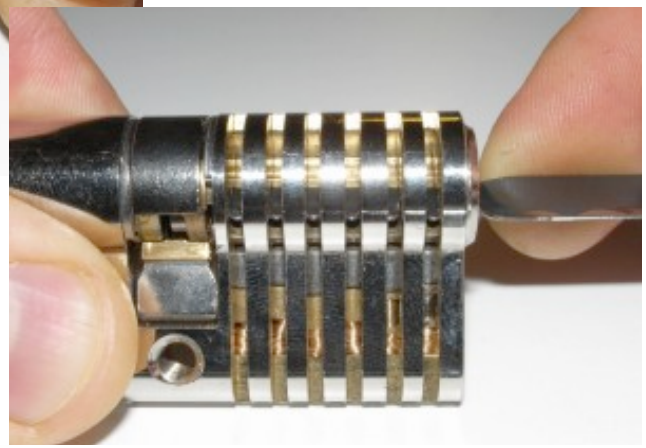

1
2
3
4
5
6
8
9
0
E
KEYWAYS
HOMESAFE

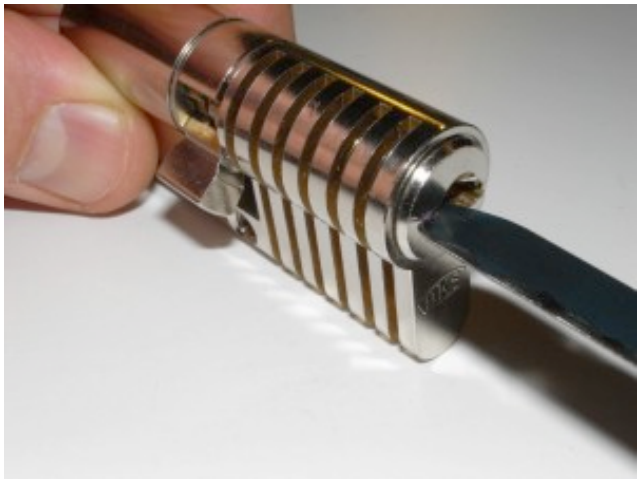






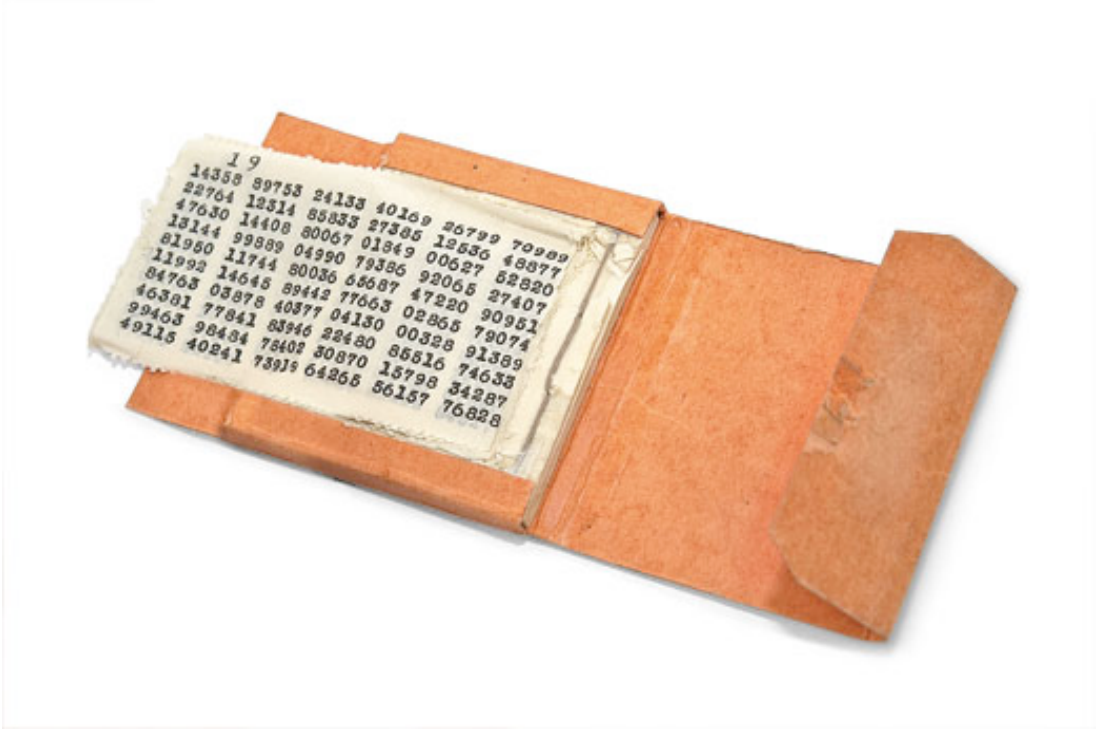




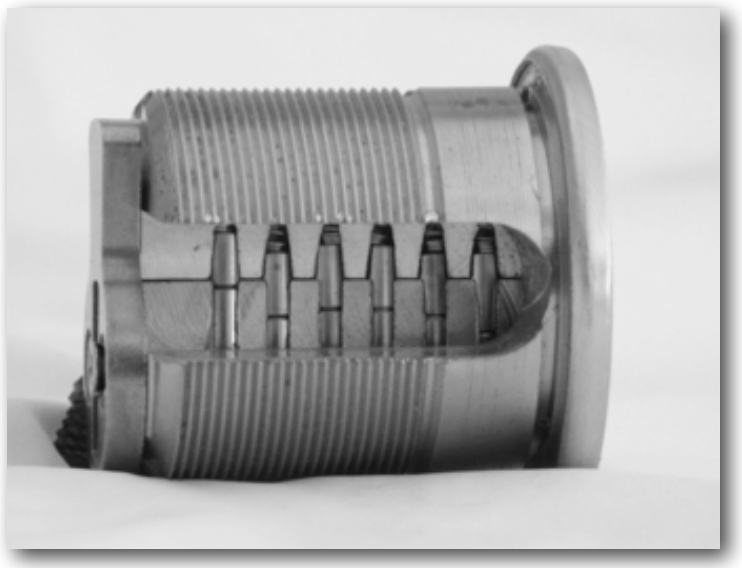


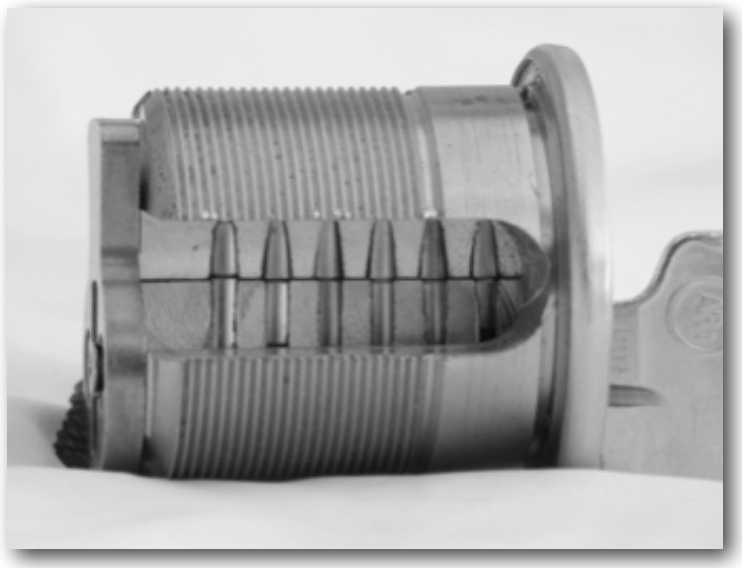
Pictures: Oliver Diederichsen

Key re-use


19
14358 89758 24133 40169 28792 70989
22764 12314 85833 27385 12536 48877
47630 14408 80067 01349 00627 52820
13144 99389 04990 79385 92065 27407
81960 11744 80036 65687 47220 90951
11992 14645 89442 77663 02855 79074
84763 03878 40377 04130 00328 91389
46381 77841 83946 22480 85816 74633
99463 98484 78402 30870 15798 34287
49115 40241 73919 64265 56157 76828

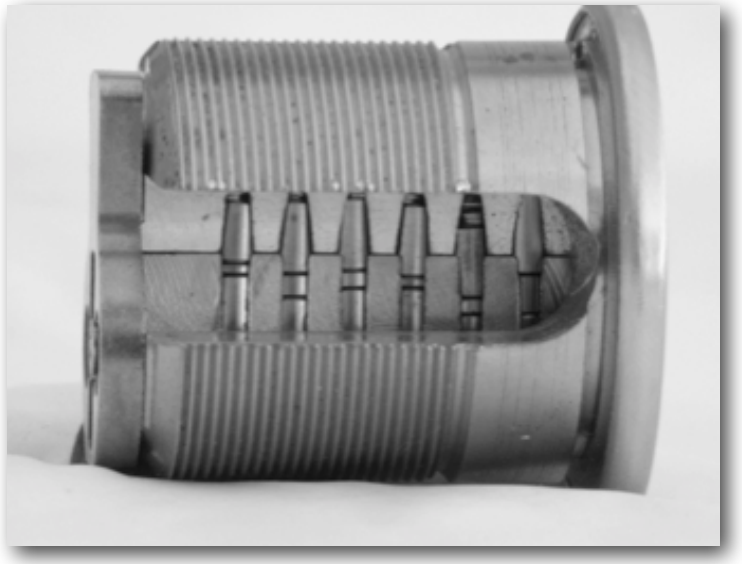
(Partial) key re-use

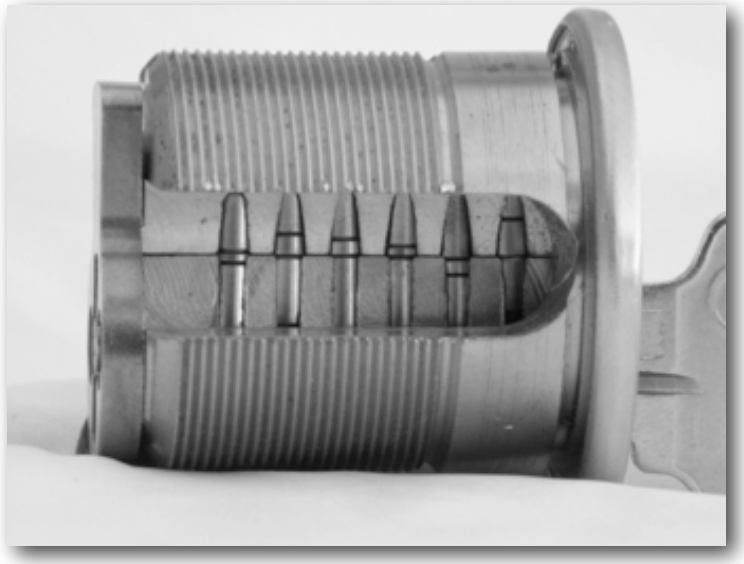




http://www.crypto.com/papers/mk.pdf

(Partial) key re-use





http://www.crypto.com/papers/mk.pdf

Root user

- Often, there is an omnipotent user
  - root
  - Domain Administrator

Root user

Using sample code

XSS vulnerability in example code provided with developer account

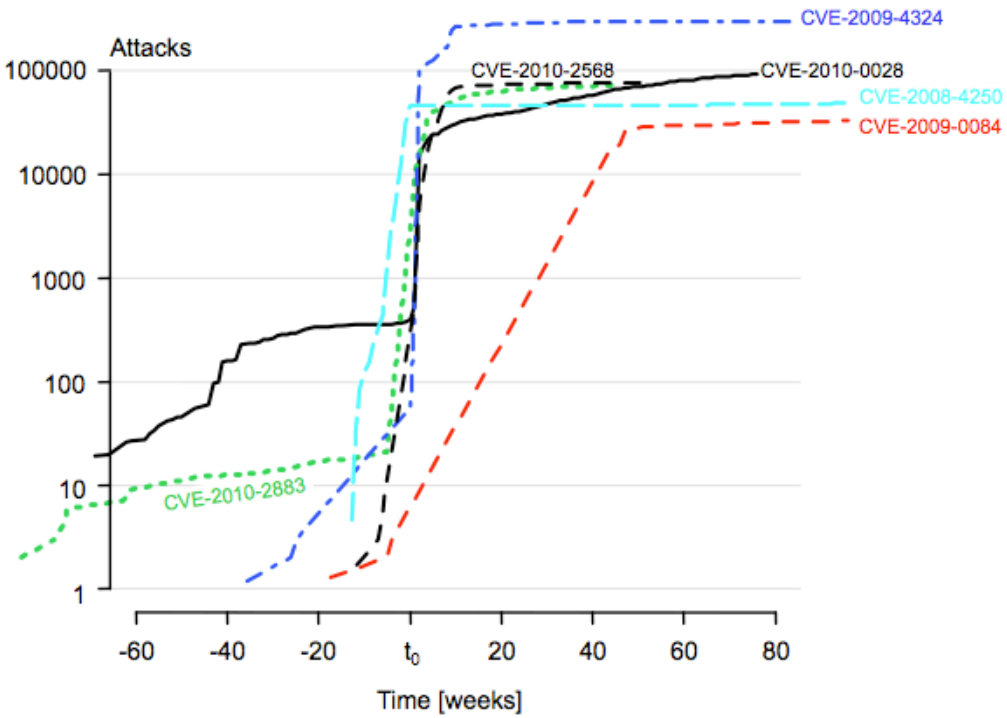
I created a test developer account. The code provided by default for the Blog collection's list page has an XSS vulnerability that allows a arbitrary javascript to be run by injecting code in a URL param. For example, displaying cookies, which could contain user data:

Using sample ‘code’

http://www.youtube.com/watch?v=Ti9S1qzPXTI

Remember showing keys?

0day



(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time = t_0).

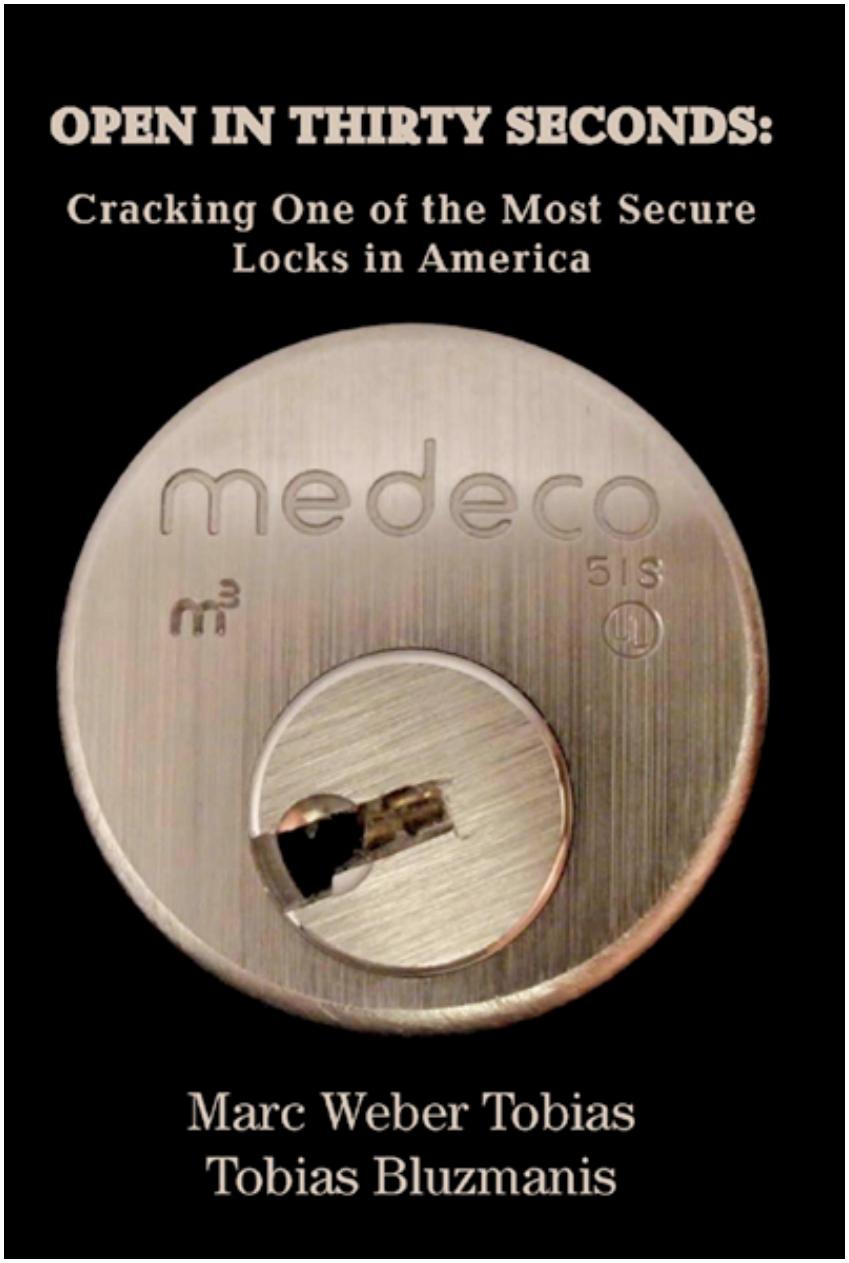
http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

Responsible disclosure

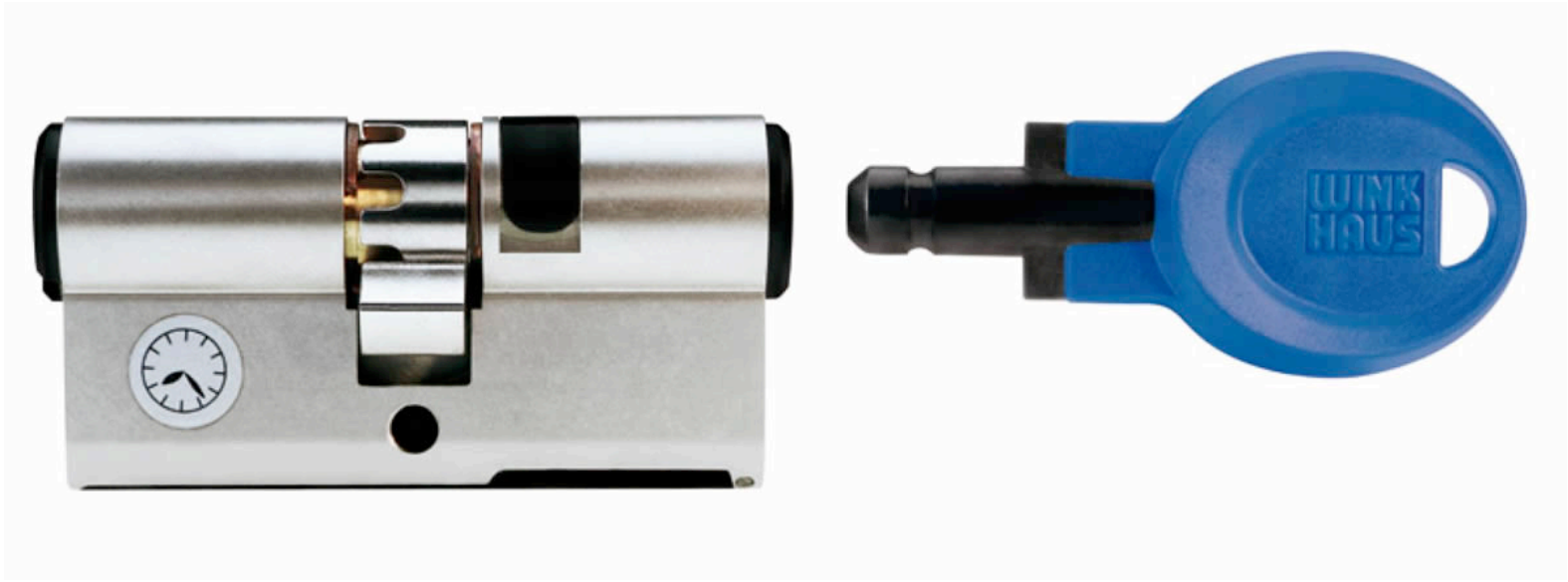
PR

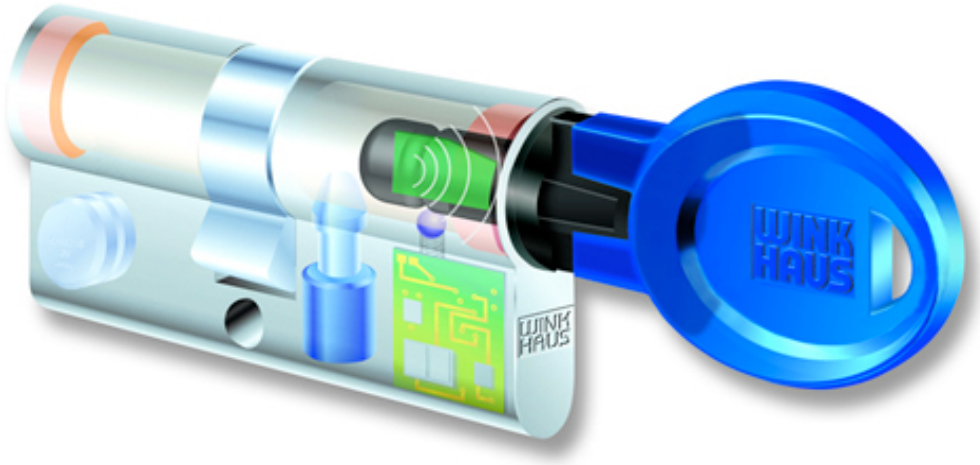
Bugs bust open 'unbreakable' Oracle 9i

Summary: *Oracle's pledge that the database software is totally secure is thrown into doubt after a number of flaws are found--including one that could let hackers take control of corporate servers.*

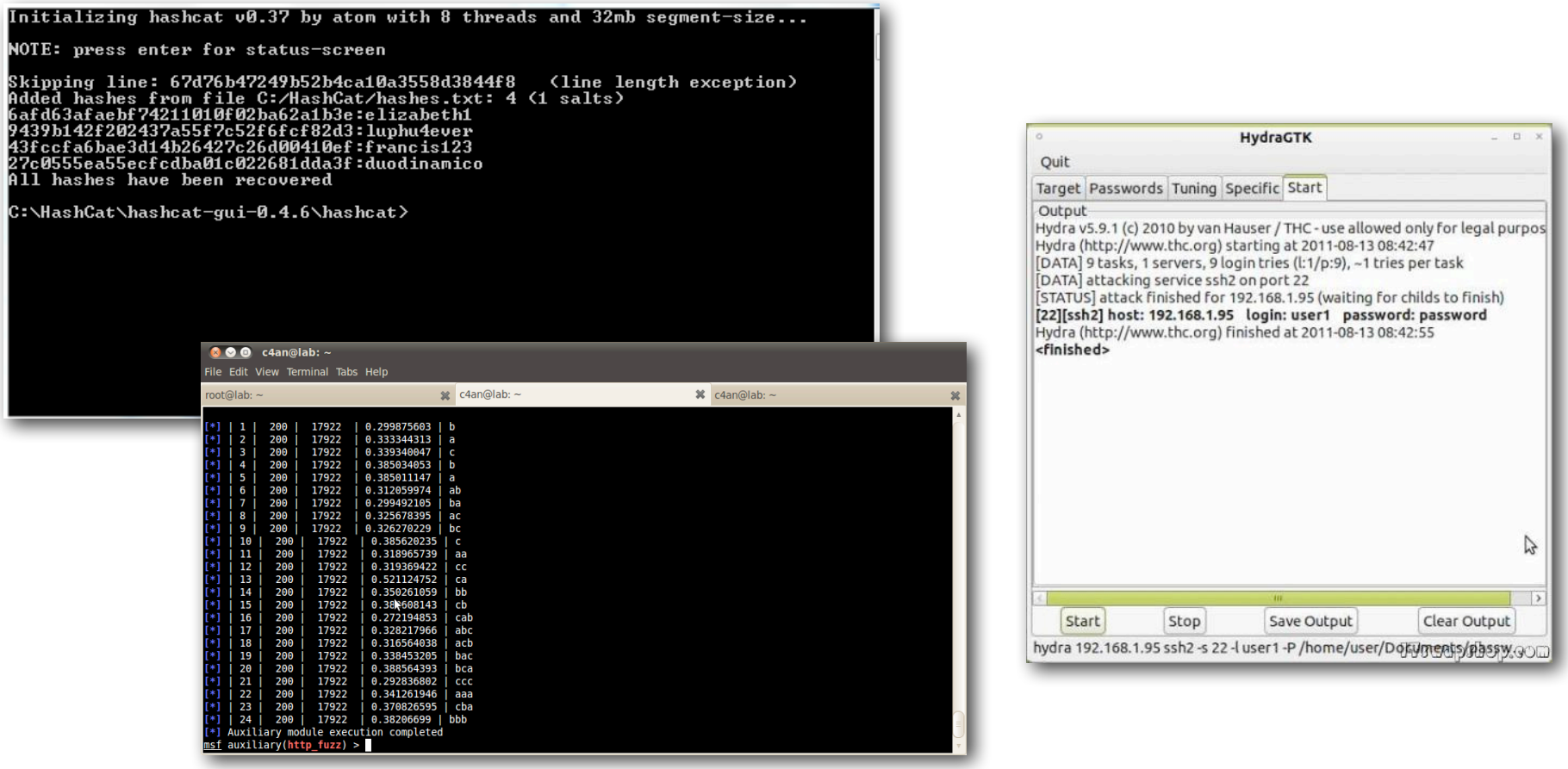

OPEN IN THIRTY SECONDS:
Cracking One of the Most Secure Locks in America
medeco
5 I S
Marc Weber Tobias
Tobias Bluzmanis


medeco

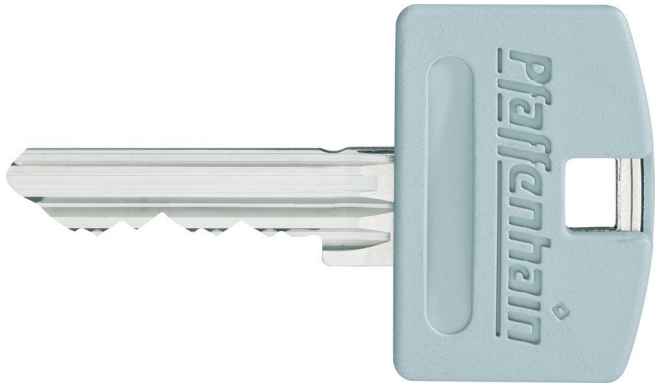

WINKHAUS

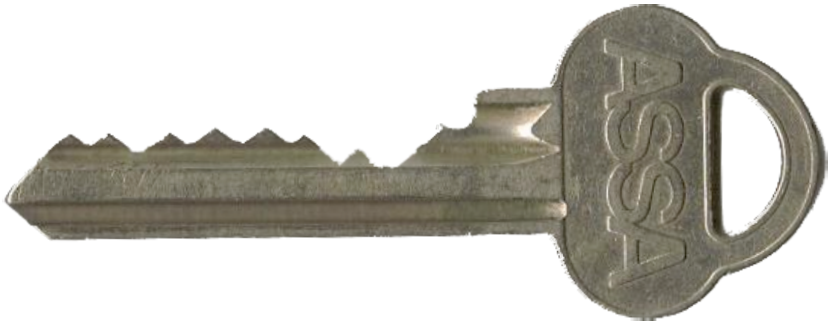

WINKHAUS
WINKHAUS

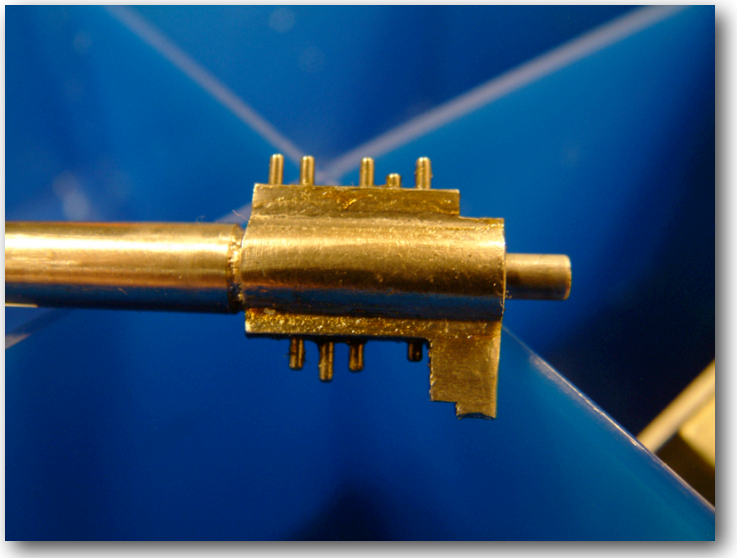
Brute force attacks



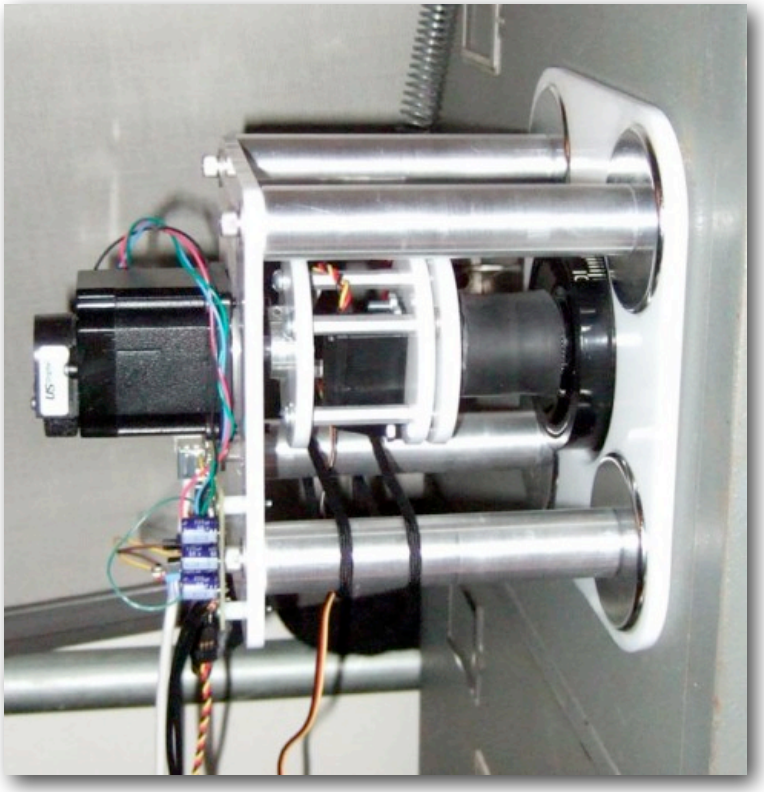
Brute force attacks



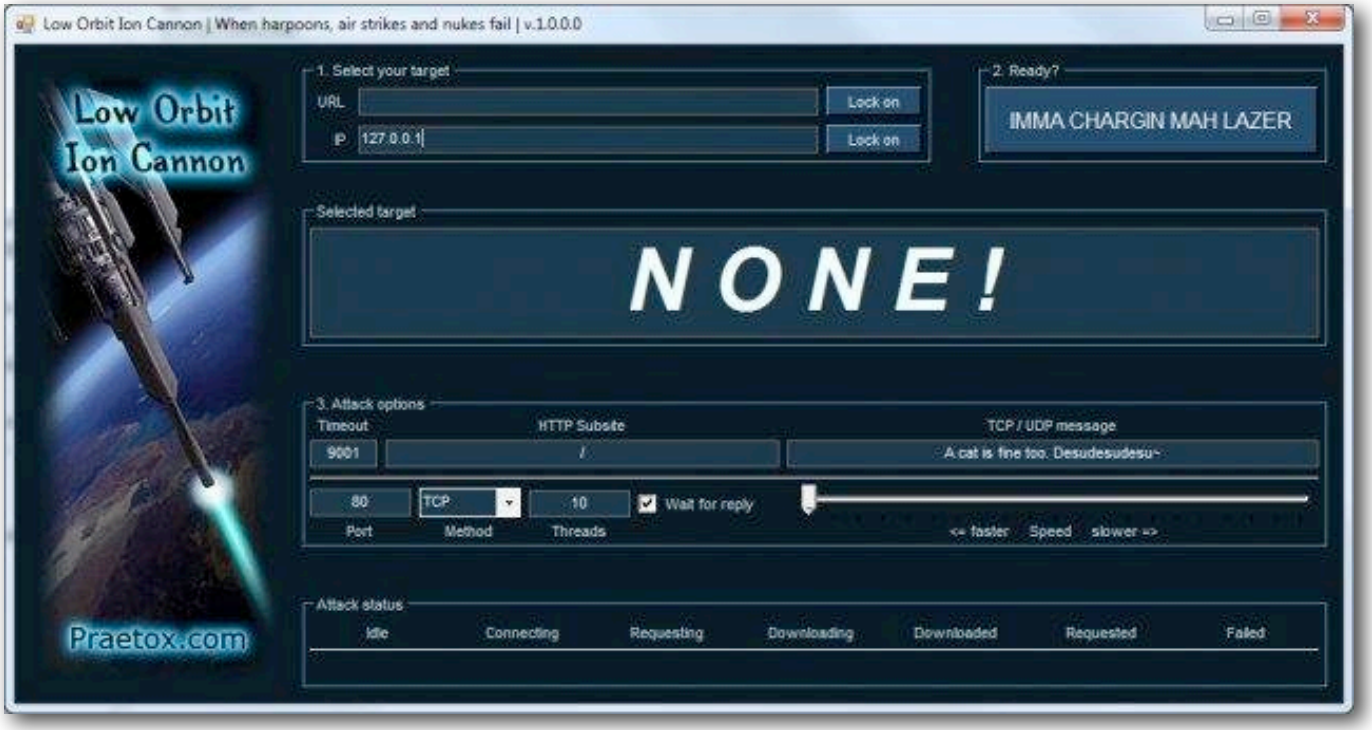




Brute force attacks



Denial of Service



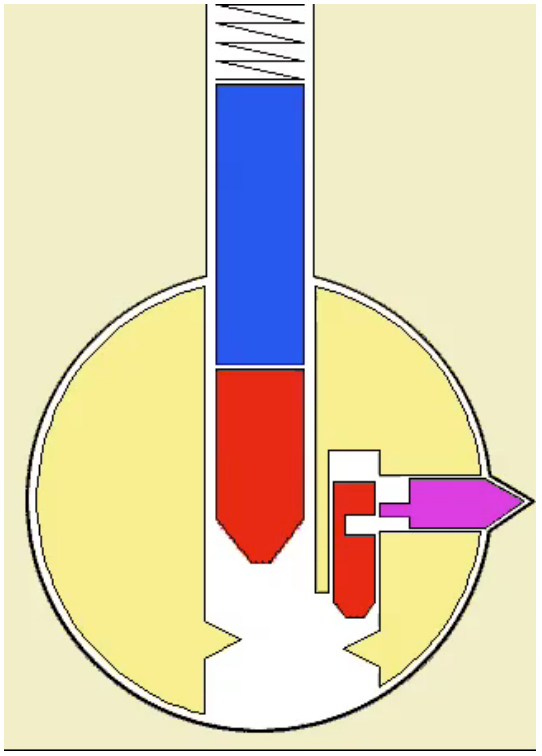
Denial of Service

Denial of Service

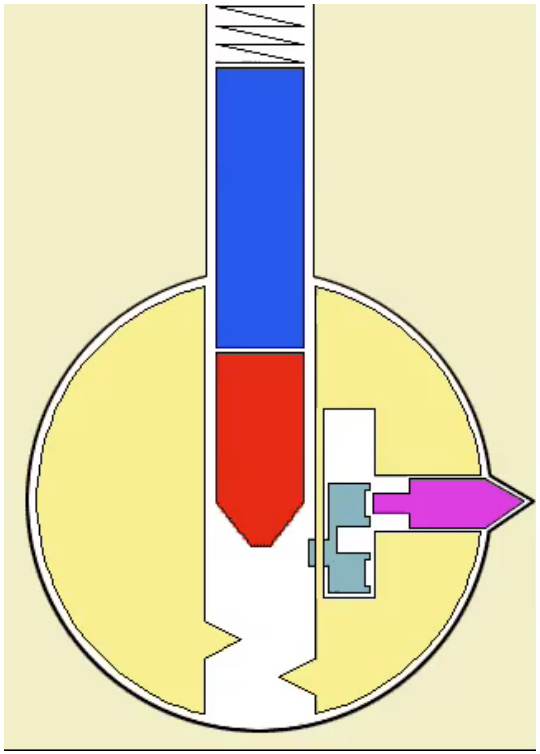
Sequential attacks

- “Unknown user” versus “Incorrect password”
- Timing attacks

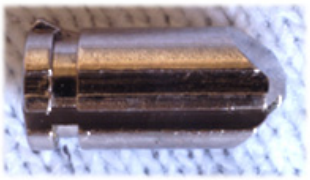
Sequential attacks

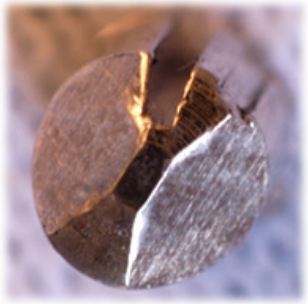


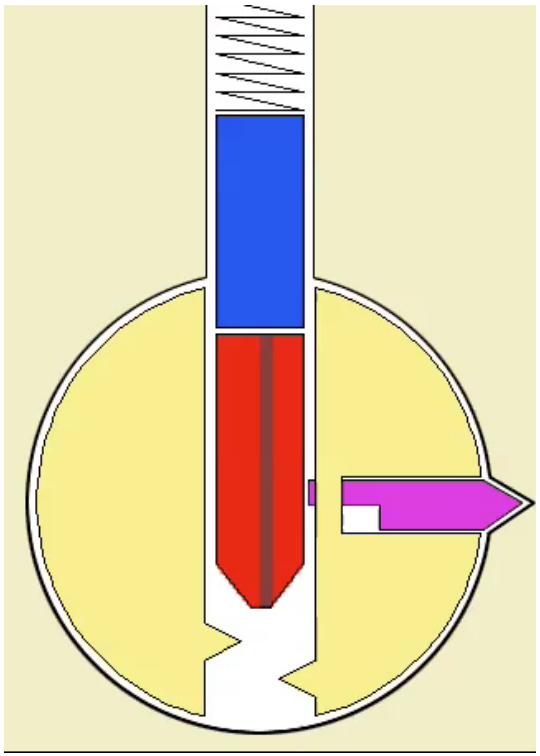
Sequential attacks



Sequential attacks





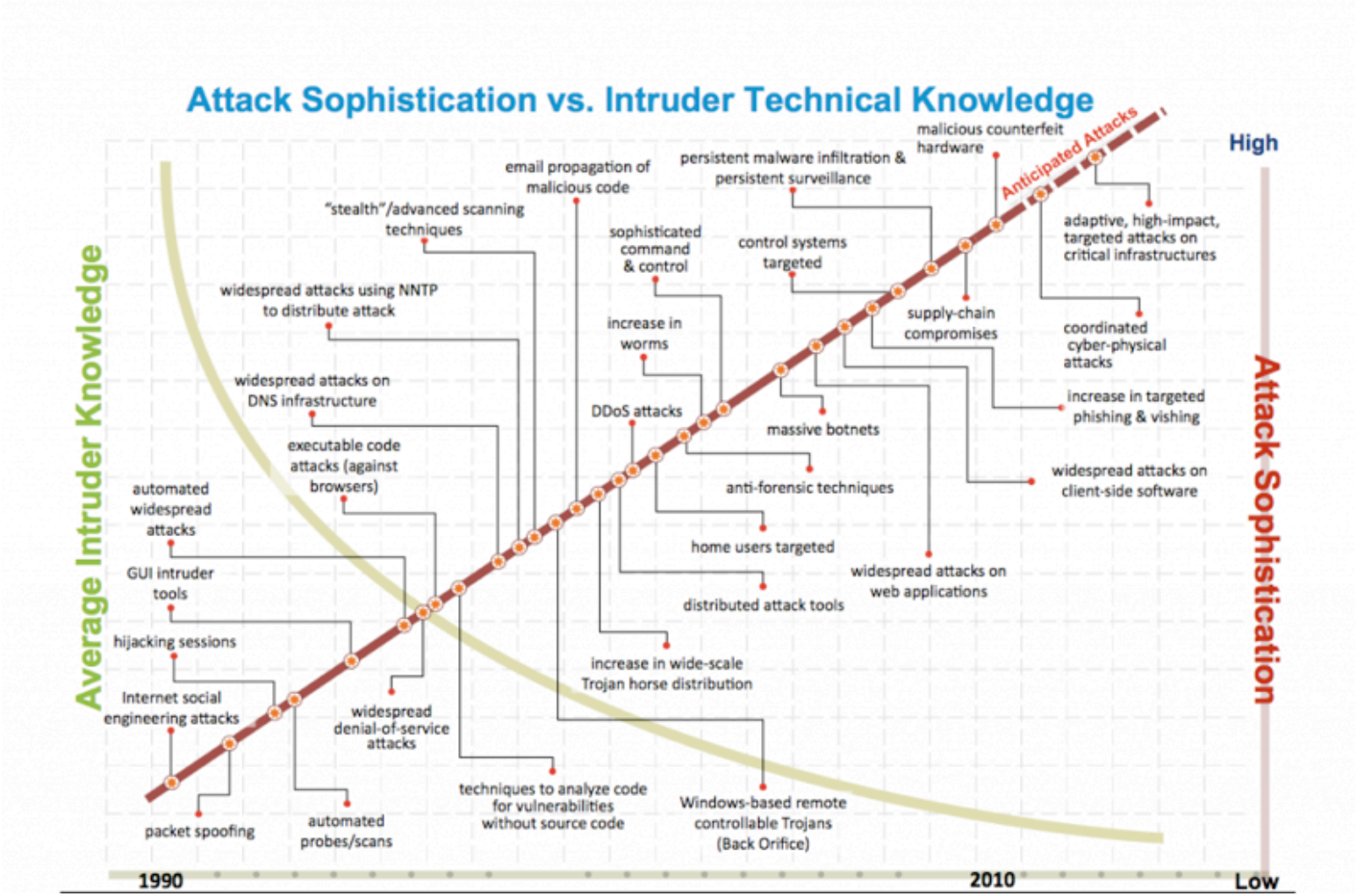


Security testing

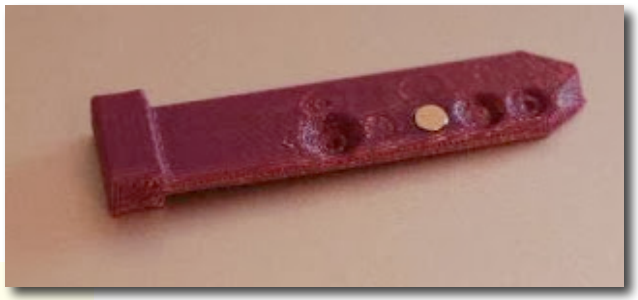
- Let an experienced security consultant look at the security?
- Use automated vulnerability scanners?
- Certification?

Certification

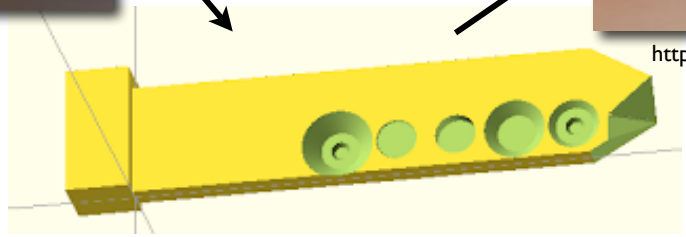
Tooling

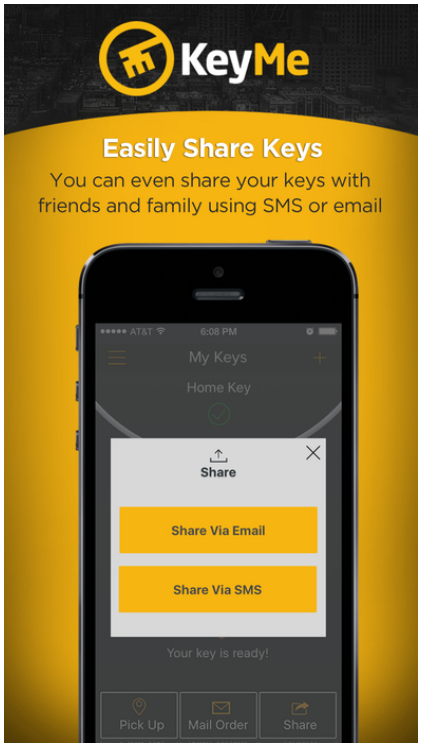

Attack Sophistication vs. Intruder Technical Knowledge
Average Intruder Knowledge
Attack Sophistication
High
Low
1990
2010
Anticipated Attacks
malicious counterfeit hardware
persistent malware infiltration & persistent surveillance
email propagation of malicious code
"stealth"/advanced scanning techniques
sophisticated command & control
control systems targeted
adaptive, high-impact, targeted attacks on critical infrastructures
widespread attacks using NNTP to distribute attack
increase in worms
supply-chain compromises
coordinated cyber-physical attacks
widespread attacks on DNS infrastructure
DDoS attacks
massive botnets
increase in targeted phishing & vishing
executable code attacks (against browsers)
anti-forensic techniques
widespread attacks on client-side software
automated widespread attacks
home users targeted
GUI intruder tools
widespread attacks on web applications
distributed attack tools
hijacking sessions
increase in wide-scale Trojan horse distribution
Internet social engineering attacks
widespread denial-of-service attacks
techniques to analyze code for vulnerabilities without source code
Windows-based remote controllable Trojans (Back Orifice)
packet spoofing
automated probes/scans

Tooling



http://www.revk.uk/2013/12/abs-lock-vs-3d-printer.html



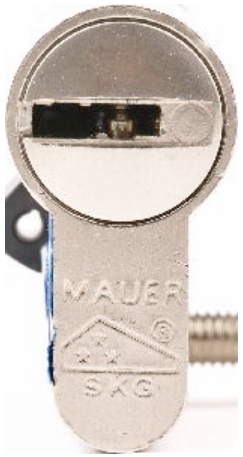


You get what you pay for

- You can’t see how secure a piece of software is
- We can’t all be security experts

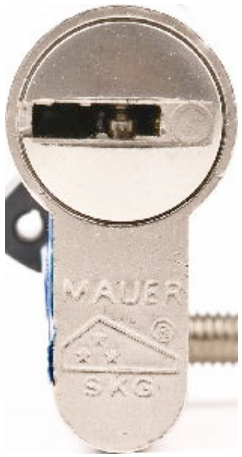
You get what you pay for

- With locks, you can see *something*
  - But does it mean anything?

You get what you pay for

- With locks, you can see *something*
- But does it mean anything?



4’49.20

3’57.00

0’40.90

0’34.31

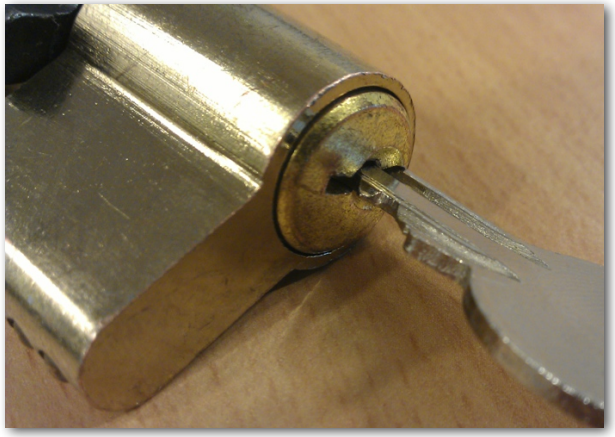
0’02.16

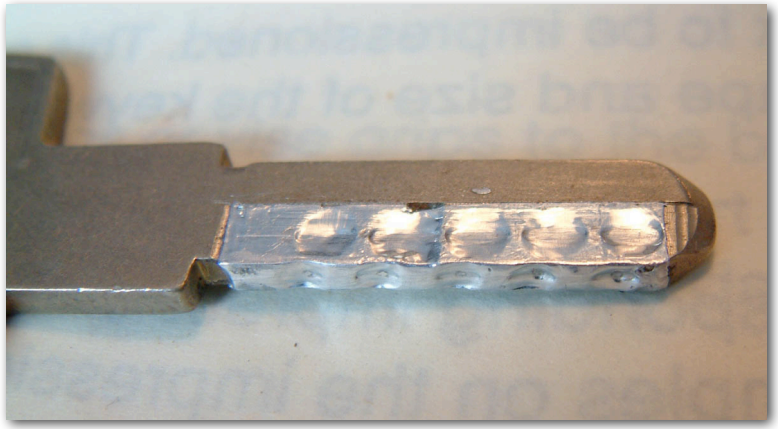
Awareness

- Always a problem..

http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Awareness



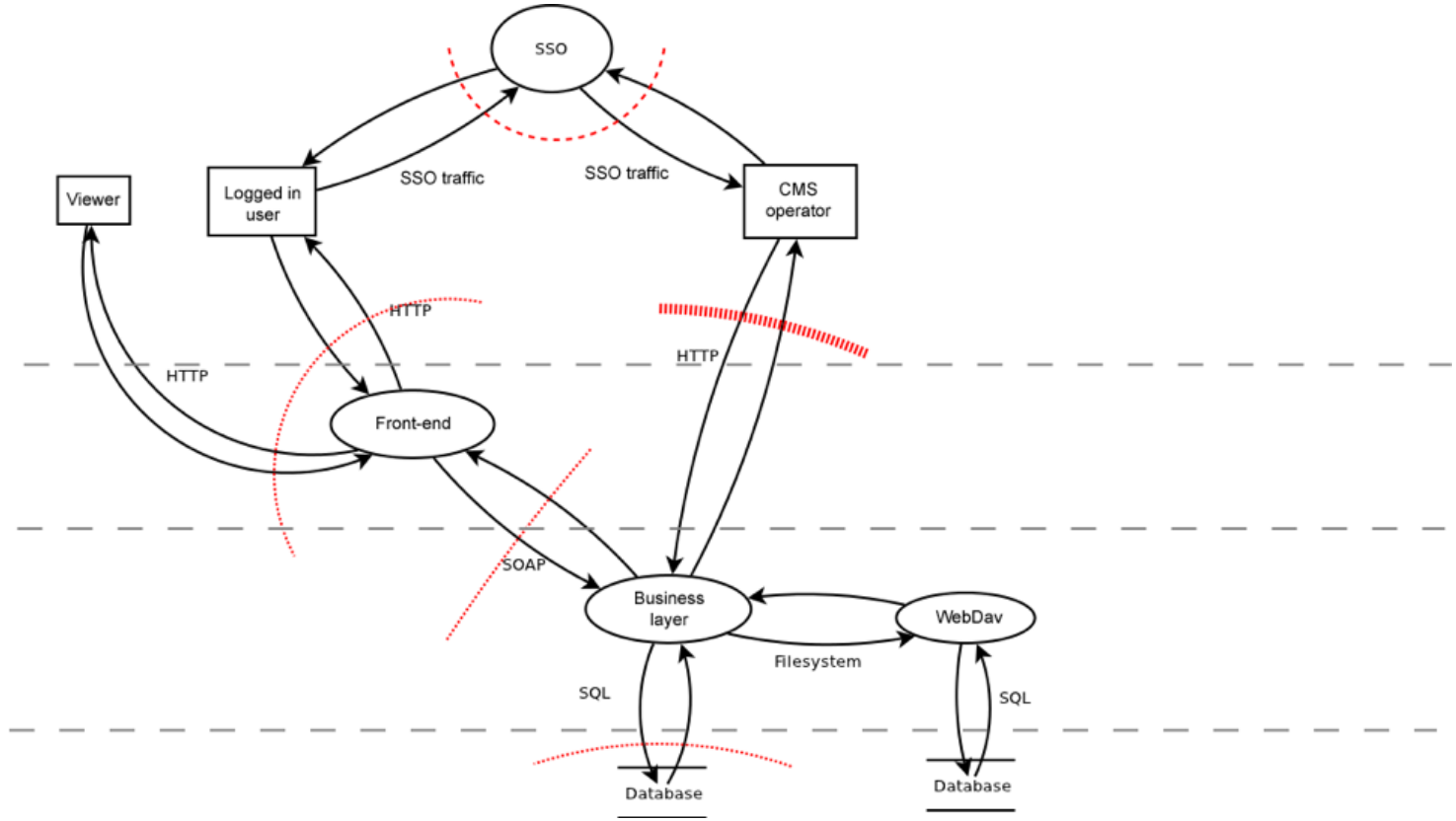


Holistic view

- You are depending on the environment
- You are as secure as the weakest link

Holistic view

Threat modeling



Thank you for your attention

Any questions?

walter@toool.nl