NICOLE RAUCH MICHAEL SPERBER

THE DAY AFTER TOMORROW

Objektorientierte und funktionale Softwareentwicklung
Refactoring von Java Legacy Code
Clean Code und Software Craftsmanship
Specification by Example und
Domain-Driven Design
Facilitation von Code Retreats und
Legacy Code Retreats

Michael Sperber

- funktionale Programmierung
- Scala, Clojure, F#, Haskell, OCaml, Erlang, Elixir, Swift
- Schulungen und Coaching
- Blog: funktionale-programmierung.de
- Entwickerkonferenz BOB bobkonf.de

Mirai IoT Botnet Description and DDoS Attack Mitigation

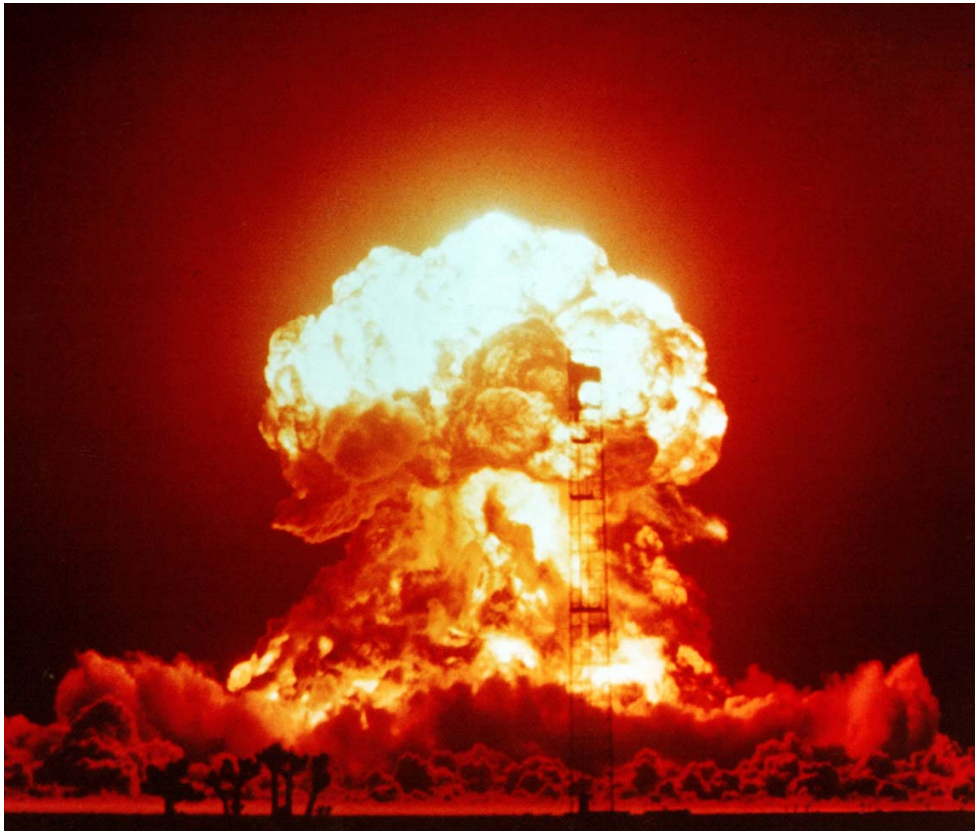
Since its inception in August of 2016, the Mirai 'Internet-of-Things' (IoT) botnet, comprised largely of Internet-enabled digital video recorders (DVRs), surveillance cameras, and other Internet-enabled embedded devices, has been utilized by attackers to launch multiple high-profile, high-impact DDoS attacks against various Internet properties and services. Mirai serves as the basis of an ongoing

https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/

HeartBleed

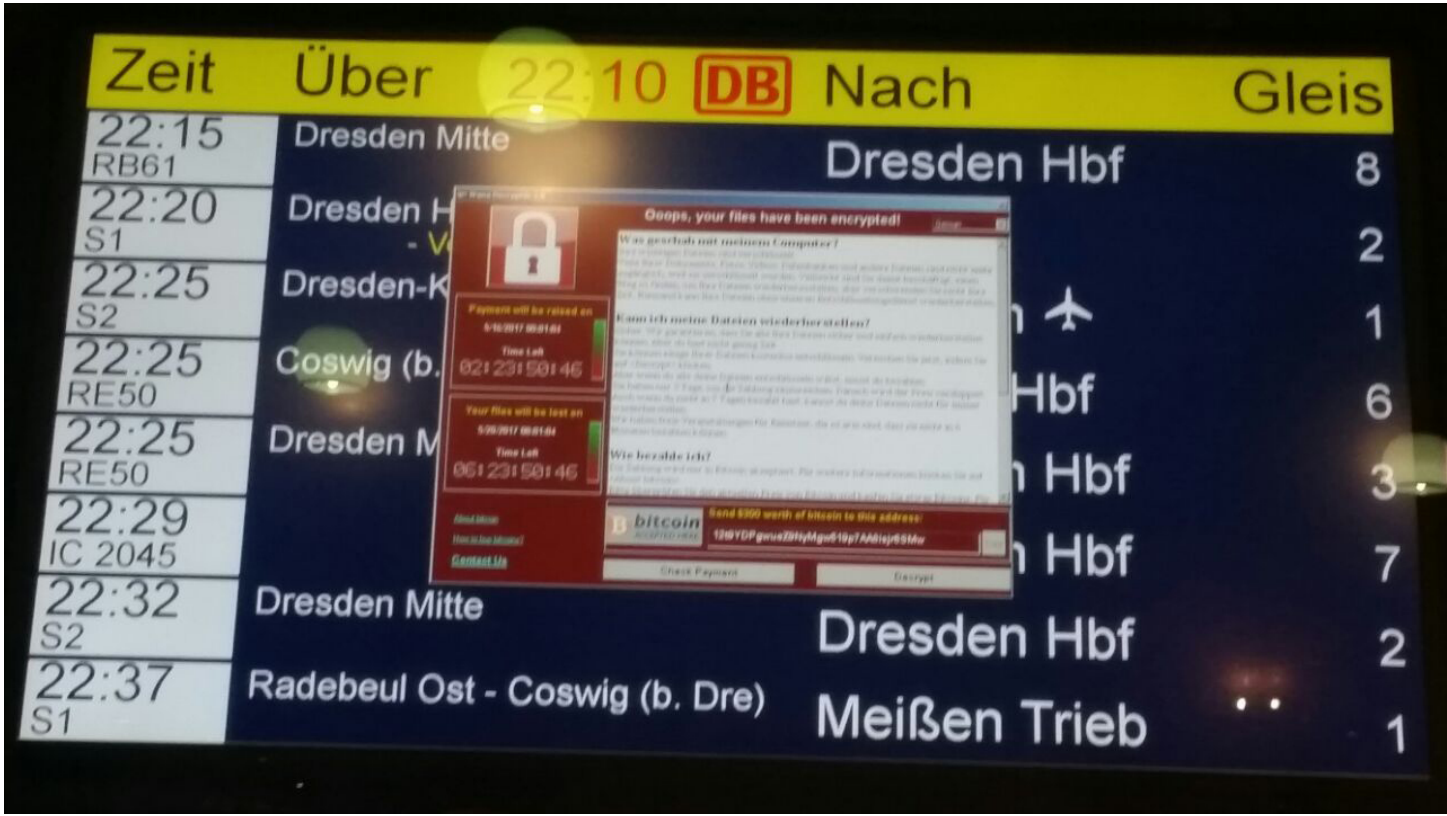
http://heartbleed.com/

CloudBleed



CLOUDFLARE

WannaCry

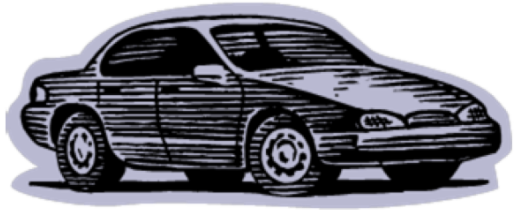

Zeit
Über
22:10
DB
Nach
Gleis
22:15
RB61
Dresden Mitte
Dresden Hbf
8
22:20
S1
2
22:25
S2
1
22:25
RE50
6
22:25
RE50
3
22:29
IC 2045
7
22:32
S2
Dresden Mitte
Dresden Hbf
2
22:37
S1
Radebeul Ost - Coswig (b. Dre)
Meißen Trieb
1
Ooops, your files have been encrypted!
Was geschah mit meinem Computer?
Kann ich meine Dateien wiederherstellen?
Wie bezahle ich?
Contact Us
bitcoin
Check Payment
Decrypt

Modern Automobile: Many Remote Attack Vectors

Mechanic

Short-range wireless

Long-range wireless



Entertainment

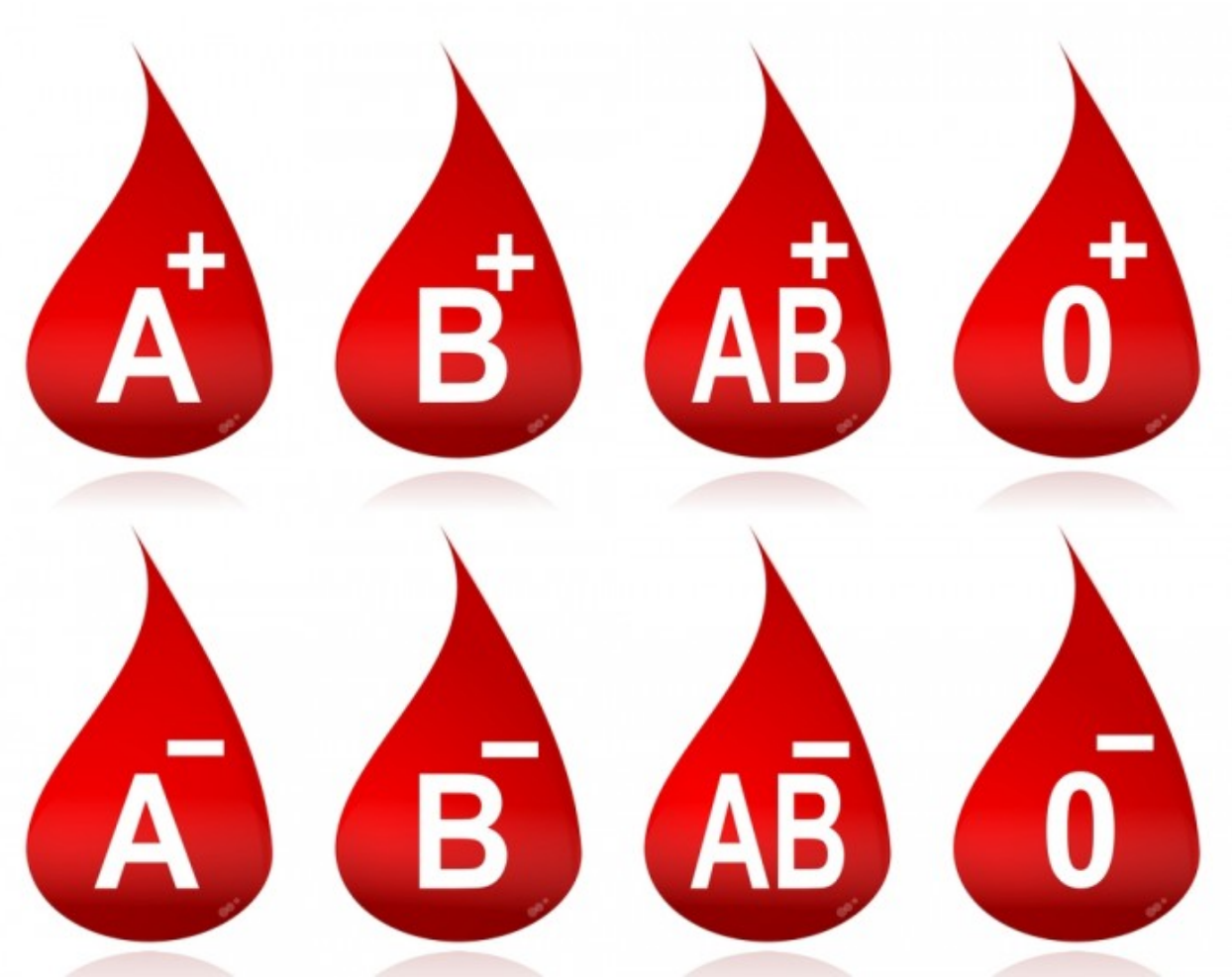
Source: Koscher, K., et al.
"Experimental Security Analysis of a Modern Automobile"

http://wp.doc.ic.ac.uk/riapav/wp-content/uploads/sites/28/2014/05/HACMS-Fisher.pdf

Korrekte Software

Intel Pentium, FDIV-Bug

Typen



CompCert

CompCert is a ***C compiler*** like Diab C

- Source: a large subset of ISO-C-99/ANSI-C language + several extensions
- Target: machine code for PowerPC, ARM and IA32 architectures

CompCert is a ***formally verified*** compiler

- Machine-assisted mathematical proof (Coq)
  - *Semantic preservation between source code and compiled code*

CompCert performs ***optimization***

- Simplification of control flow and wise use of data resources
  - Controlled and non aggressive optimization

AIRBUS

http://projects.laas.fr/IFSE/FMF/J3/slides/P05_Jean_Souyiris.pdf

Tools

- Coq
- Isabelle
- Agda
- Idris
- ATS
- F*
- ACL2
- Liquid/
  Dependent Haskell

Eigenschaften

```
∀xs: List a

xs = rev (rev xs)

rev [x] = [x]

rev (append xs1 xs2) =
     append (rev xs2) (rev xs1)
```

Algebra

$$a + b = b + a$$

$$a + (b + c) = (a + b) + c$$

$$a \times (b + c) = (a \times b) + (a \times c)$$

Eigenschaften

Formal Verification of Floating-Point RTL at AMD Using the ACL2 Theorem Prover

David Russinoff

Matt Kaufmann

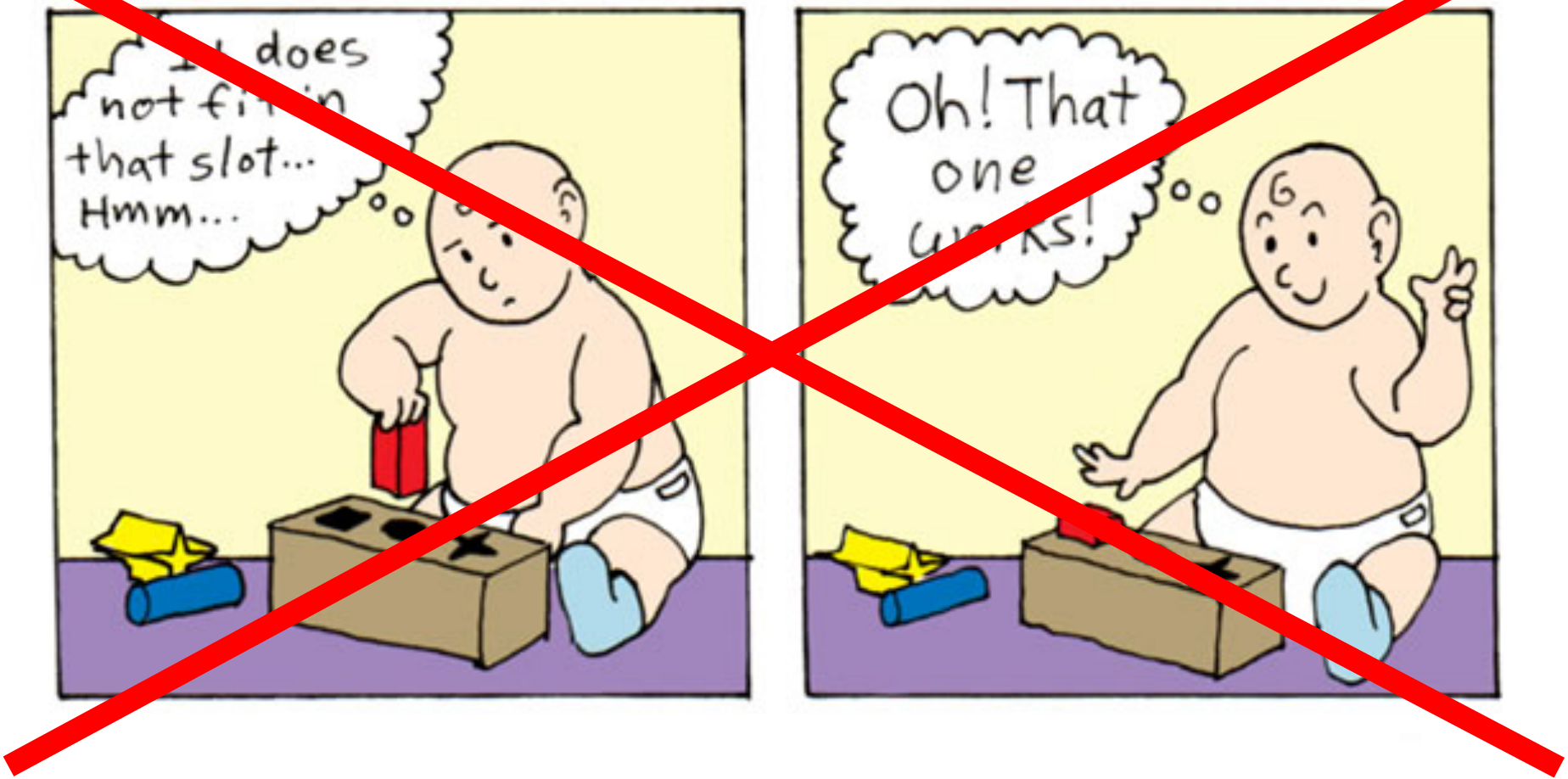
Eric Smith

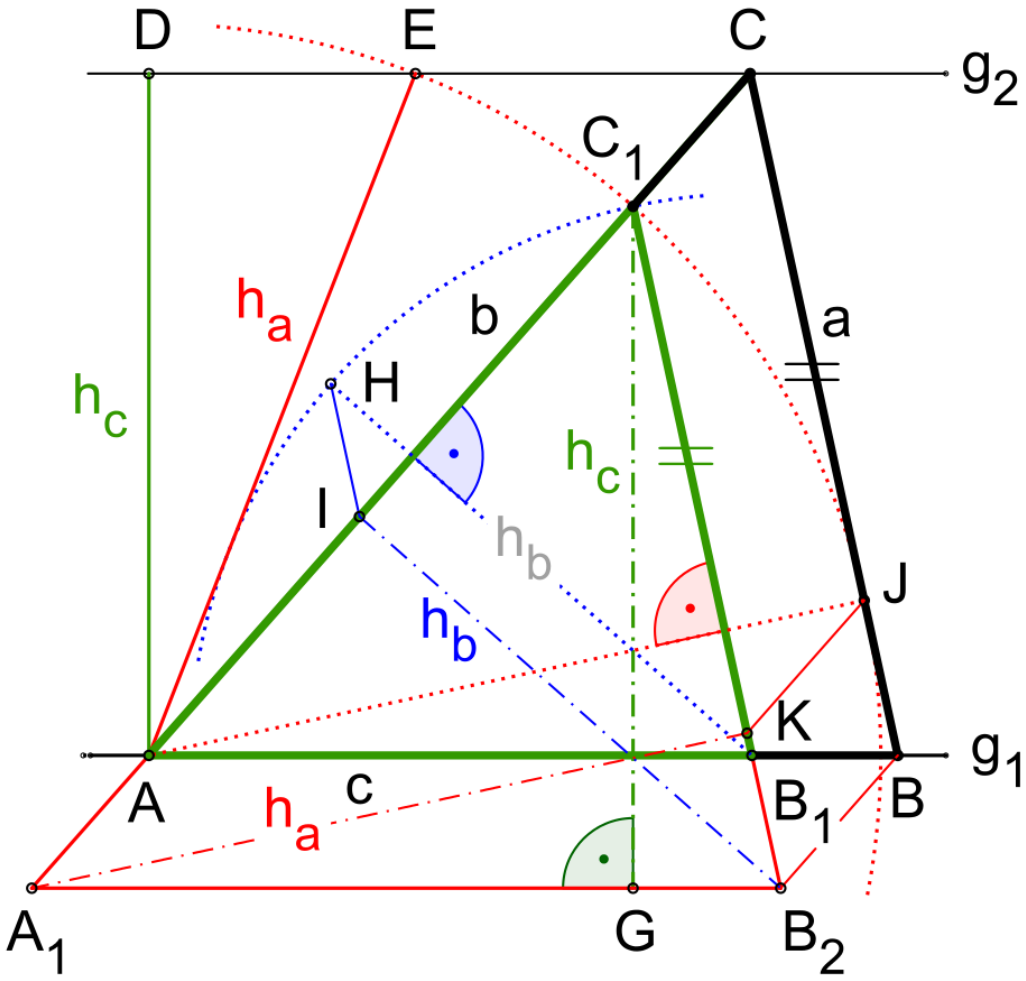
Robert Sumners

Advanced Micro Devices, Inc., Austin, TX

Phone: 512-602-6741, Fax: 512-602-6970, E-mail: david.russinoff@amd.com

http://www.russinoff.com/papers/paris.ps


does
not fit in
that slot...
Hmm...
Oh! That
one


D
E
C
g_2
C_1
h_a
b
a
h_c
H
h_c
I
h_b
h_b
J
K
g_1
A
c
h_a
B_1
B
A_1
G
B_2

The seL4 Microkernel

Security is no excuse for poor performance!

The world's first operating-system kernel with an end-to-end proof of implementation correctness and security enforcement is available as open source.

https://sel4.systems/


THE DAY
AFTER TOMORROW

Tomorrow?

QuickCheck: A Lightweight Tool for Random Testing of Haskell Programs

Koen Claessen
Chalmers University of Technology
koen@cs.chalmers.se

John Hughes
Chalmers University of Technology
rjmh@cs.chalmers.se

(International Conference on Functional Programming, 2000)

Today!

Program by Design