HISOLUTIONS

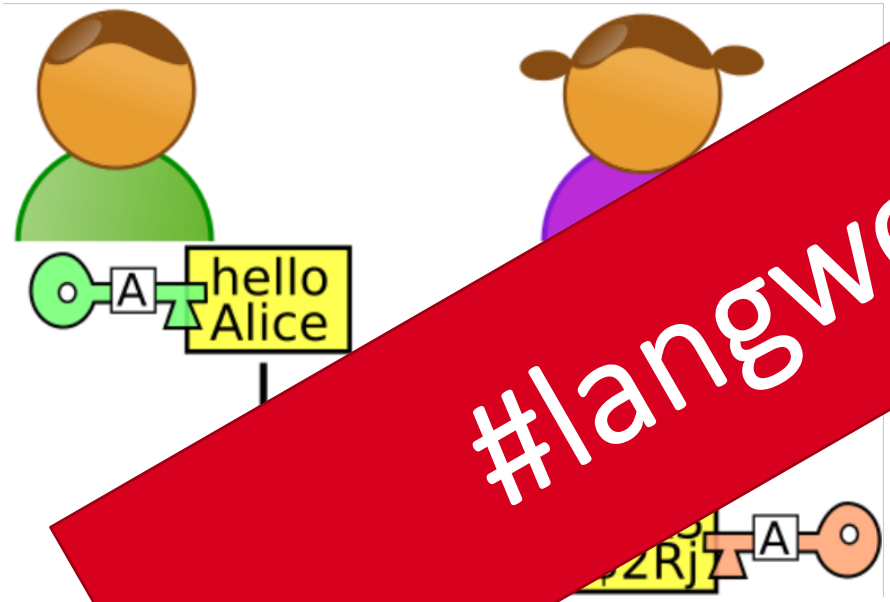
Spectre & Co. für Normalsterbliche

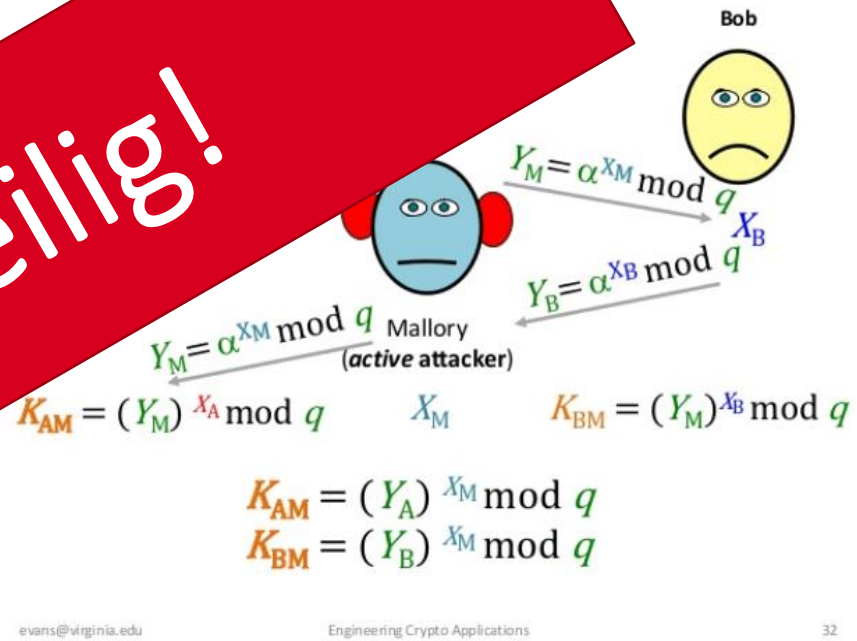
Wie man Muggels Schwachstellen erklärt

ISD 2018

David Fuhr/Frank Rustemeyer

Das Märchen von Alice und Bob





#langweilig!

David Fuhr

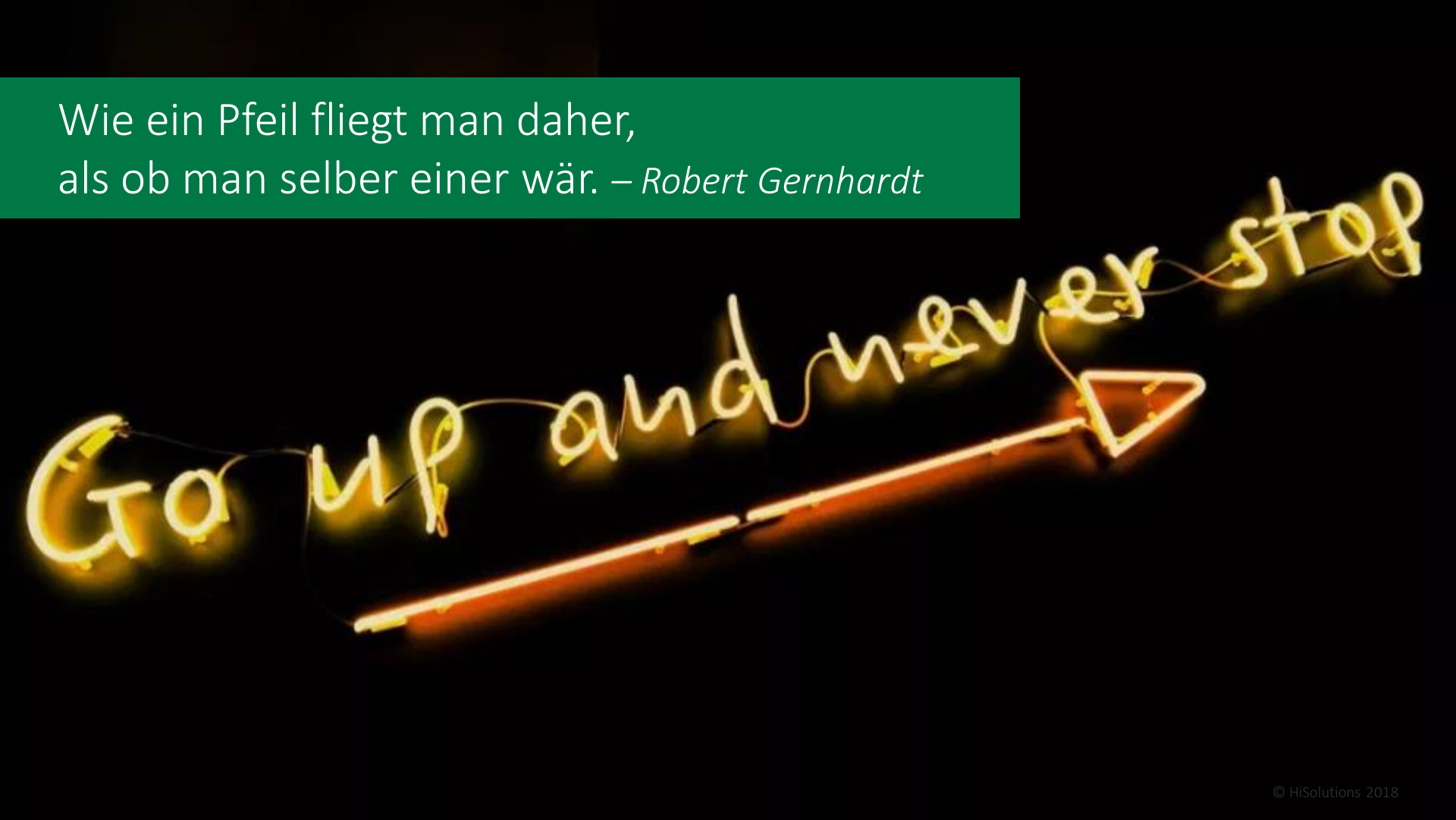
Head of Research, HiSolutions AG

Therapeut/Coach

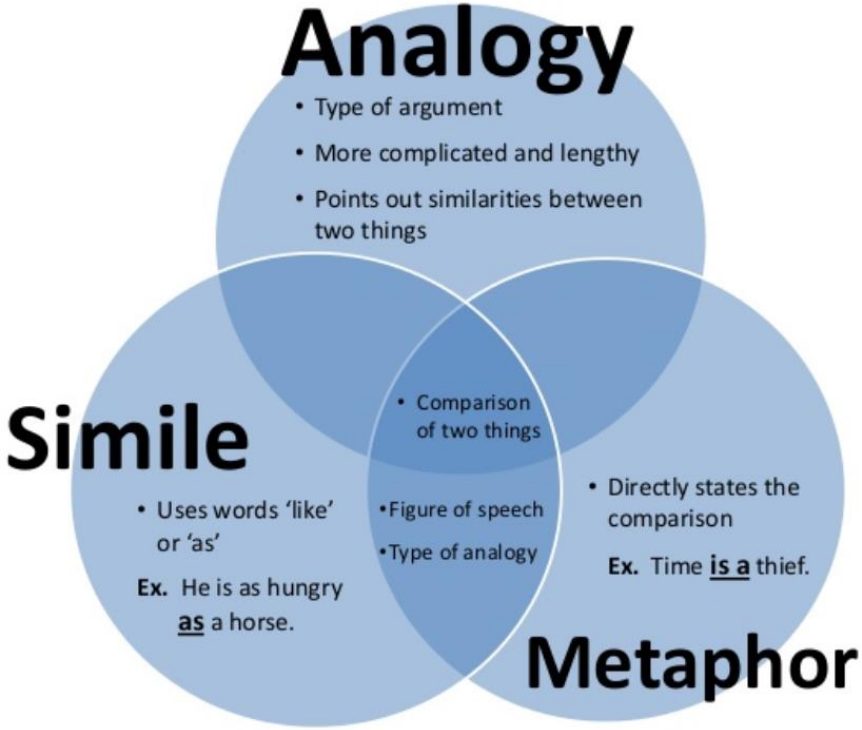
Vater

Grenzenlos neugierig

Wie ein Pfeil fliegt man daher,
als ob man selber einer wär. – *Robert Gernhardt*



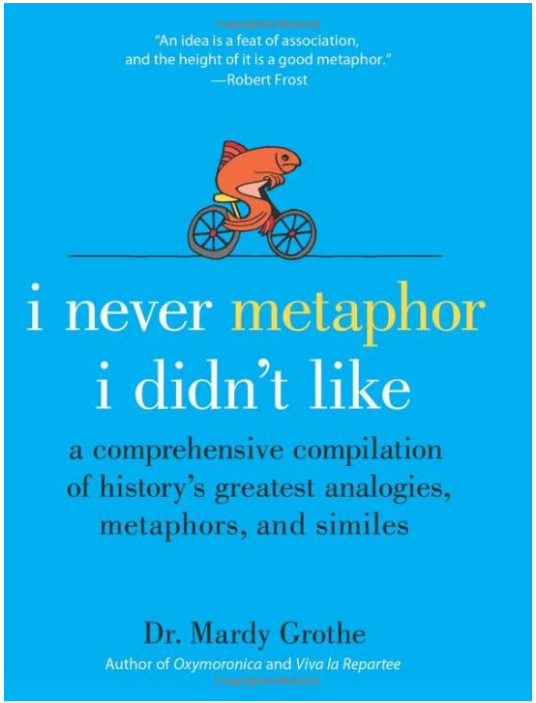
Vergleich, Metapher, Analogie



https://aspergerhuman.wordpress.com/2017/04/06/metaphor-analogy-simile-fun-with-language/

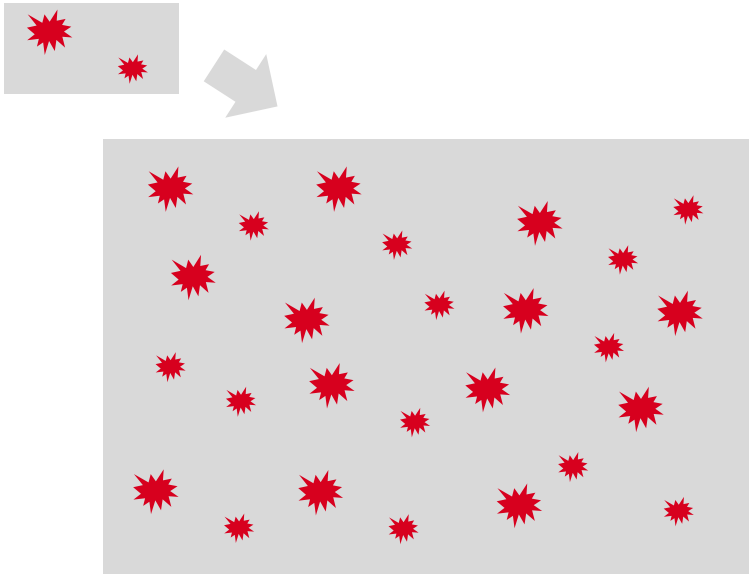
Wofür sind Metaphern gut?

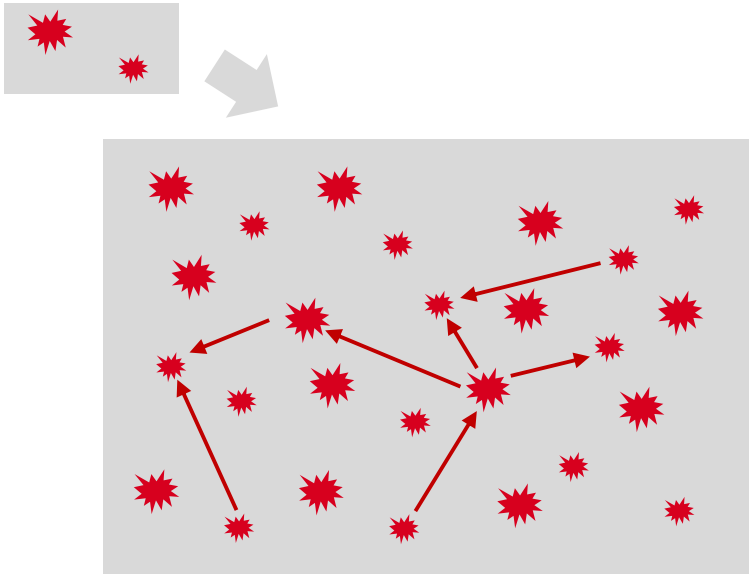
- Einfach(er)
- Motivierend
- Explorativ



Google’s services are powered by 5,000 times more lines of code than the space shuttle

Consequences of Complexity





An increase in the complexity of IT does not only mean that there are more security flaws, it also means that there are *more complicated* security flaws.

Meltdown & Spectre

Series of vulnerabilities published starting January, 2018

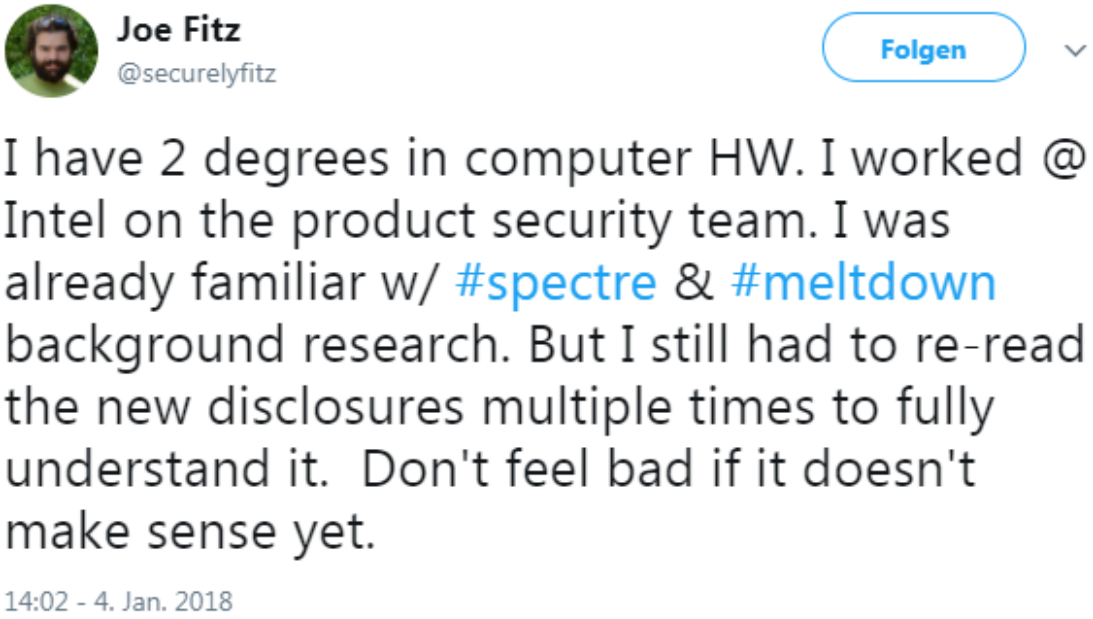
Problems in microprocessor architecture, with exploits potentially compromising business applications

Highly complex things happening within microprocessors that had hitherto rarely even been glanced at by security professionals

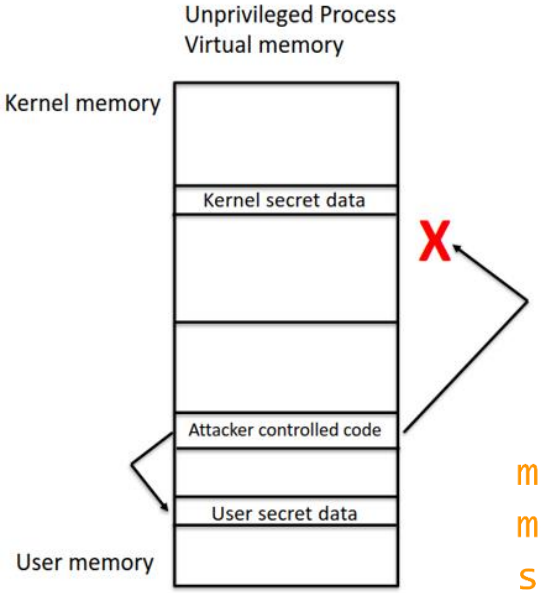
Security consultants were severely challenged to understand, even more so to communicate these vulnerabilities

No chance for mere mortals / muggles…

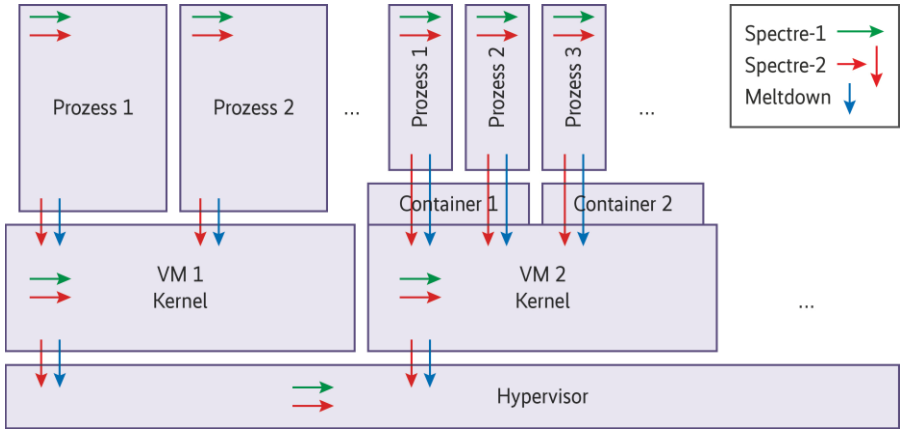
Ein Hardware Security Trainer and Researcher so:



Vizualisations…



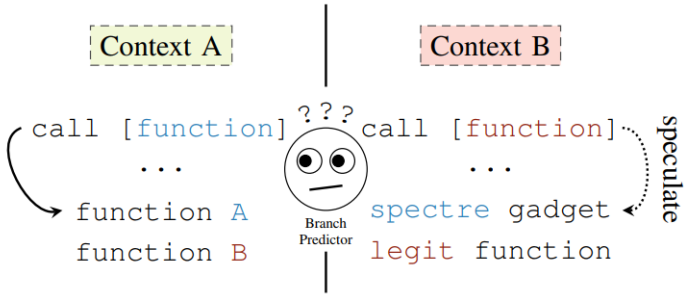
Source: https://www.renditioninfosec.com/2018/01/updated-spectre-and-meltdown/



Source: https://www.heise.de/select/ix/2018/2/1517770391119975

```
meltdown:
mov al, byte [rcx]
shl rax, 0xc
jz meltdown
mov rbx, qword [rbx + rax]
```

Source: https://meltdownattack.com/

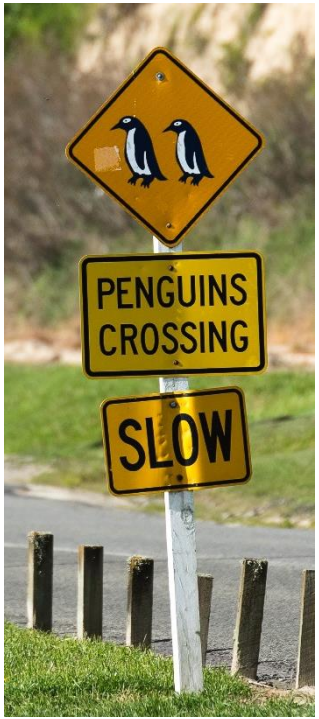


Source: https://spectreattack.com/spectre.pdf

Meltdown and Spectre Explained By a Security Expert

- This class of vulnerabilities exploits features of modern CPUs called „out-of-order-execution“ and „speculative execution“.
- Instructions are pipelined within the CPU. Instructions have different latencies, so the CPU begins executing „later“ instructions before the current instruction is completed *for performance reasons*.
- Sometimes, this involves assumptions about the flow of the program (branch predictions).
- As a consequence, instructions may be executed before it is made certain that they should be. This includes subsequent checks for the separation of user space and kernal space.
- If it turns out that an instruction must not be executed, *theoretically* all effects of the premature („transient“) execution are „rolled back“.
  A rolled-back instruction *should* not have any detectable leftovers on the system.
- However, they *do* have side-effects, e.g. on memory caching. By the use of *side-channel* attacks, an attacker can retrieve information about the transient instructions.
- This mechanism can be exploited to read data from memory that is meant to be protected.

Idea



It is easier to convey complex information by using images, metaphors and examples.

Ideally, complex technical procedures can be explained by analogies that the audience is *familiar* with.

Challenge: Can we explain Meltdown and Spectre without talking about microprocessors at all?

An instruction walks into a bar.
No, wait, it doesn’t!

The Bar Metaphor

- Our computer is a bar, with a barkeeper processing different customers‘ orders.
- Customers may want to keep their drinking habits private.
- We are a malicious customer who wants to gain private information illigitimately.

I. Meltdown

What is Bob‘s Favourite Drink?

- Bob won‘t tell us – he wants to keep his favourite drink secret.
- We secretly follow him into a bar.
- Bob goes to the counter and orders something, but we can‘t hear what is being said.
- While the bartender starts preparing the drink, Bob spots us and quickly leaves the bar.
- We go to the bartender and order all the drinks from the menu.
- The bartender accepts the offer and promptly serves us a Gin Tonic, which he happens to have prepared for a customer that just left. He then starts preparing the other drinks.
- We conclude that Bob has a good taste.

What is Bob‘s Favourite Drink?

- Bob won‘t tell us – he wants to keep his favourite drink secret.
- We secretly follow him into a bar.
- Bob goes to the counter and orders something, but we can‘t hear what is being said.
- While the bartender starts preparing the drink, Bob spots us and quickly leaves the bar.
- We go to the bartender and order all the drinks from the menu.
- The bartender accepts the offer and promptly serves us a Gin Tonic, which he happens to have prepared for a customer that just left. He then starts preparing the other drinks.
- We conclude that Bob has a good taste.

Modern CPUs use their capabilities to do things in advance, speculatively, in order to increase speed.

What is Bob‘s Favourite Drink?

- Bob won‘t tell us – he wants to keep his favourite drink secret.
- We secretly follow him into a bar.
- Bob goes to the counter and orders something, but we can‘t hear what is being said.
- While the bartender starts preparing the drink, Bob spots us and quickly leaves the bar.
- We go to the bartender and order all the drinks from the menu.
- The bartender accepts the offer and promptly serves us a Gin Tonic, which he happens to have prepared for a customer that just left. He then starts preparing the other drinks.
- We conclude that Bob has a good taste.

Modern CPUs use their capabilities to do things in advance, speculatively, in order to increase speed.

Sometimes, things prepared in advance are made obsolete by security restrictions.

What is Bob‘s Favourite Drink?

- Bob won‘t tell us – he wants to keep his favourite drink secret.
- We secretly follow him into a bar.
- Bob goes to the counter and orders something, but we can‘t hear what is being said.
- While the bartender starts preparing the drink, Bob spots us and quickly leaves the bar.
- We go to the bartender and order all the drinks from the menu.
- The bartender accepts the offer and promptly serves us a Gin Tonic, which he happens to have prepared for a customer that just left. He then starts preparing the other drinks.
- We conclude that Bob has a good taste.

Modern CPUs use their capabilities to do things in advance, speculatively, in order to increase speed.

Sometimes, things prepared in advance are made obsolete by security restrictions.

However, by cycling through potential data and checking the speed of the responses, an attacker can find out things that were meant to be kept secret.

II. Spectre 1

What is Bob‘s Favourite Drink?

- Bob won‘t tell us – he wants to keep his favourite drink secret.
- We secretly follow him into a bar.
- When the barkeeper sees Bob queueing, he starts preparing his usual order, knowing him as a regular customer.
- Bob spots us behind him and intentionally orders something different.
- We go to the bartender and order all the drinks from the menu.
- The bartender accepts the offer and promptly serves us an Altbier, which he happens to have prepared for a customer that just left. He then starts preparing the other drinks.
- We conclude that Bob is from Düsseldorf.

What is Bob‘s Favourite Drink?

- Bob won‘t tell us – he wants to keep his favourite drink secret.
- We secretly follow him into a bar.
- When the barkeeper sees Bob queueing, he starts preparing his usual order, knowing him as a regular customer.
- Bob spots us behind him and intentionally orders something different.
- We go to the bartender and order all the drinks from the menu.
- The bartender accepts the offer and promptly serves us an Altbier, which he happens to have prepared for a customer that just left. He then starts preparing the other drinks.
- We conclude that Bob is from Düsseldorf.
- Poor Bob #längsteleitungderwelt

Spectre is similar to Meltdown, but exploits the computer‘s prediction about the program flow, especially if that prediction turns out to be false.

III. Meltdown Remedies

Countermeasures

- KPTI (Kernel Page-Table Isolation):
  Drinks for privileged customers may not be served from the same stock as drinks for non-privileged customers. Semi-finished drinks may not be used for orders of the other customer group.

- PCID (Process Context Identifiers):
  During preparation, drinks get a label with the customer group. Semi-finished drinks may only be used for customers of the same group.

IV. Perspectives

Metaphors Show/Hide Different Perspectives

- Abstractions – like hiding of perspectives – is one of the dangers of a metaphor:
  - Important details can get lost
- … but also one of their strengths:
  - Focus can be set
  - Interest/curiosity can be guided
  - Similarities with other structures can become visible

→ This is what the best of modern Maths is based on!

Meltdown & Spectre Revisited

What Is the Real World Impact of Meltdown & Spectre?

- E.g. in Cloud Computing
- Different question => different abstraction => different metaphor

→Enter the house (appartment building)

- Apartments := applications (or VMs, which are similar to apps on our abstraction level)
- Housekeeping/janitor/facility service := OS / kernel

- Claim: Only tenants can enter apartments. Facility has a key to be used in emergencies. Tenants are not allowed to look inside or enter other apartments.

- Question: What is the impact of Meltdown and of Spectre in this model/metaphor?

Meltdown

- Nobody but facility staff is allowed in the FM office with all the paperwork etc.
- But they check too late! So one tenant can enter for a moment before he is thrown out.
- He doesn‘t have time to read much, but has photographic memory,
- so he will manage to redraw a lot of the things he saw on the walls afterwards, including secrets like what rent others are paying.
- He cannot enter any other apartments, nor can he tamper with FM or other tenants‘ stuff.

Spectre

- Our evil tenant would like to know what his neighbor watches on TV.
- He calls FM into his neighbors apartment several times with a fake call: „My favourite show is not running, can you check my TV please?“
- After he while, he calls FM under his real name and asks „The Simpsons are not running, could you please check“?
- If the answer is „&%/%/(„§“!§ AGAIN!!!“ – gotcha. Otherwise, keep calling…
- We can thereby „read“ secrets from other apartments without entering,
- e.g., from another VM at a Cloud hoster!

Weiteres Beispiel

- OCSP*-Stapling

* Online Certificate Status Protocol

Grenzen und Fallstricke von Metaphern

Risiken

- Sometimes, the analogy chosen does not work for specific technical aspects.
  In our example, it is very difficult to explain „Spectre 2“ by finding an adequate example (making our barman prepare something that isn‘t actually on the menu).

- Masking relevant parts

- Sometimes, exploring the metaphor may result in conclusions that do not mirror the „actual“situation – we „get lost“ in the metaphor.

Abstraktionen

- Wir benutzen ständig Abstraktionen, wie ein Prozessor/Chip/... angeblich funktioniert
- und hätten moderne Computer ohne diese Kultur-"Technik" gar nicht entwickeln können
- Aber Abstraktionen sind auch die Wurzel vieler Schwachstellen (vgl. Thomas Dullien, Weird Machines, 2017):

→ In realen Maschinen sind "Weird Machines" versteckt, die man ausnutzen kann.

Mach! Alles! Richtig!

Metaphern und ihre richtige Verwendung sind wichtig

- fachlich
- pädagogisch
- für das Recruiting

Empfehlungen

Recommendations

- If you need to convey a technical complexity to non-technical people, spend some thoughts on using an analogy that they are familiar with.

- Consider including variants and make sure you know how far the analogy will carry you, and where its limits are.

- Only once the principle is understood, provide a „translation“ (*The barkeeper is our computer*).

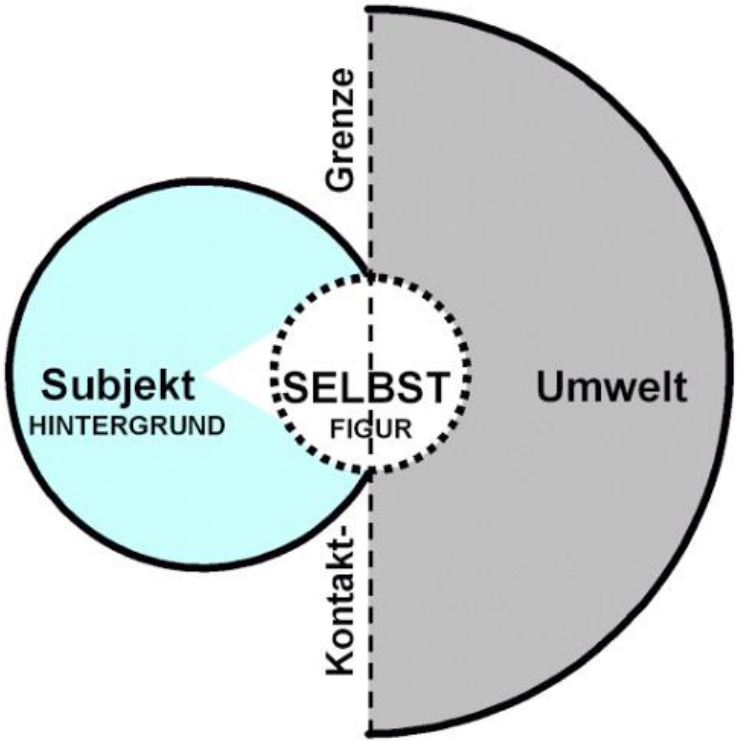
Analogies and metaphors will help you make people **understand** and **remember**, if properly used.

Etwas größer gedacht

Security als Erziehung

- ~~Security der Erziehung~~
- Erziehung zur Security
- Securityerziehung
- Security = Erziehung / Security als Erziehung

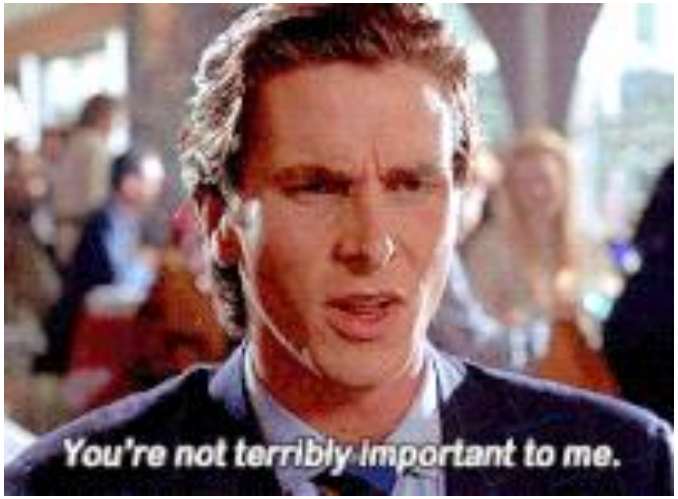
Gestalt – Kontakt findet an der Grenze statt

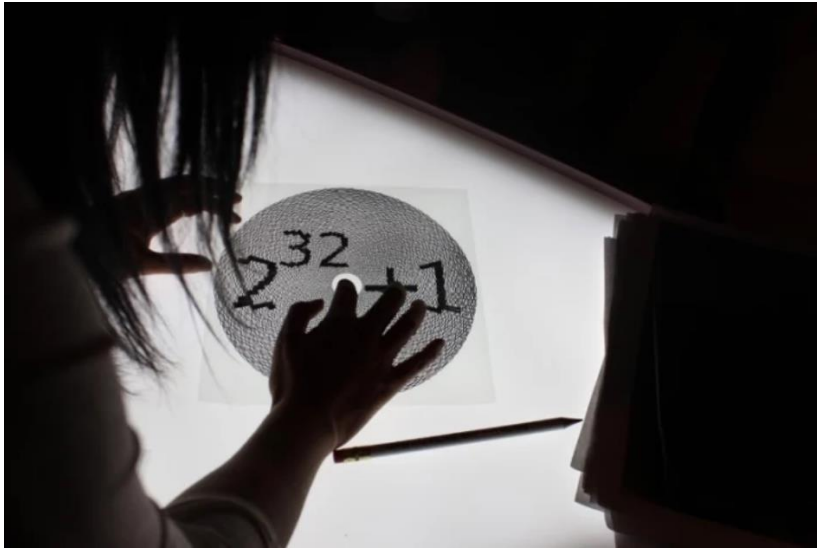


http://andreas-mensch.blogspot.com/2010/10/das-sein-im-blickwinkel-der.html

Think even bigger

Woran merke ich, dass eine Branche wirklich wichtig ist?





Wo ist das Security-Museum?


WE
FOUNDERS

David Fuhr
fuhr@hisolutions.com

HISOLUTIONS

Bouchéstraße 12 | 12435 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com