

Debugging - Bug stories

Steven Costiou

RMoD / Inria Lille - Nord Europe

September 2022

steven.costiou@inria.fr

Evil coffee machines

**Debugging: The 9 indispensable rules for
finding even the most elusive software and
hardware problems**, David J. Agans, 2002
(p.34)

Evil coffee machines

Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems, David J. Agans, 2002



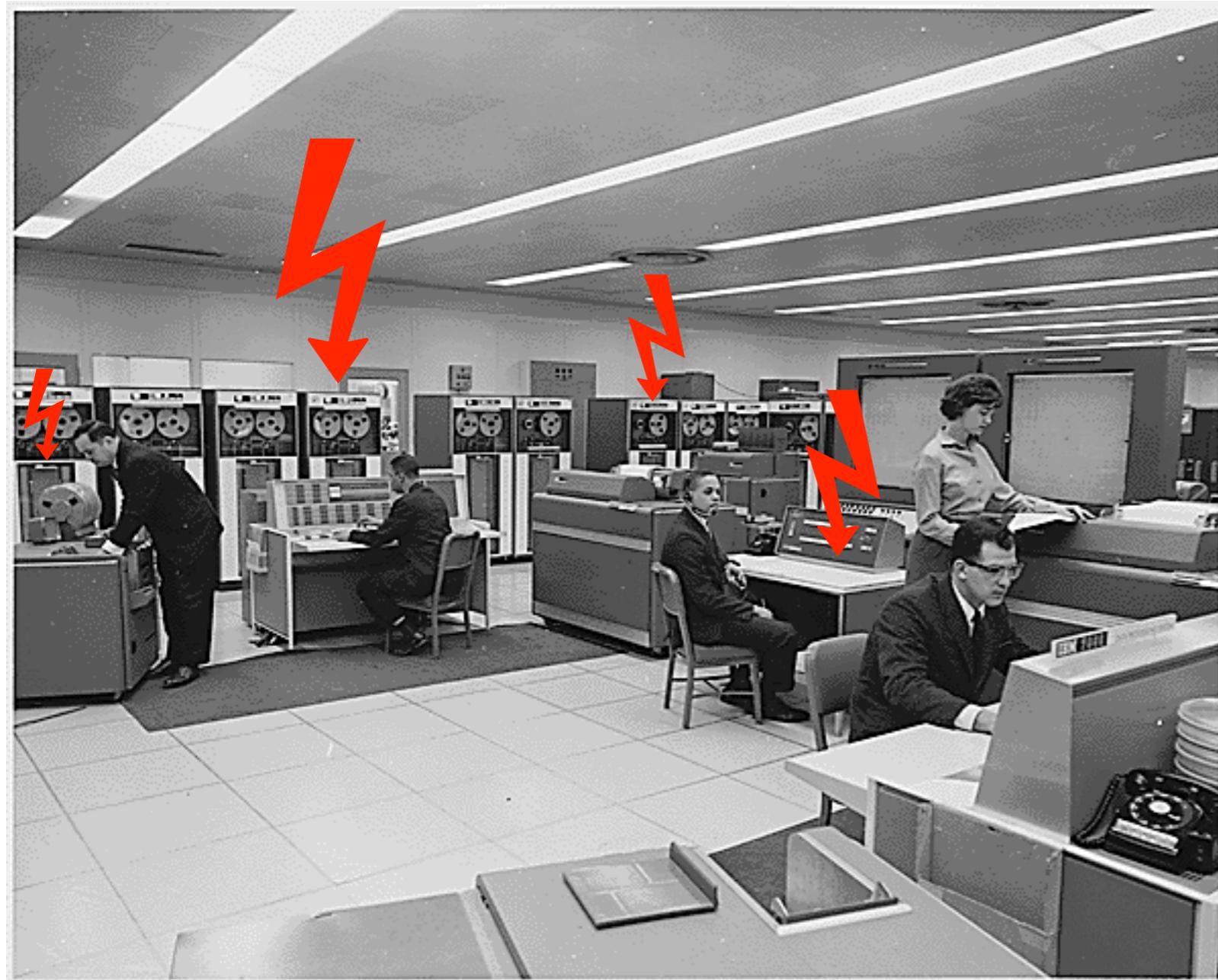
Crashing every day
around the same time



Mainframe computer (source: wikipedia)

Evil coffee machines

Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems, David J. Agans, 2002



Mainframe computer (source: wikipedia)

Crashing every day
around the same time



But in different places
in the program

Evil coffee machines

Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems, David J. Agans, 2002



Around the same time, in the cafeteria...



Crowded cafeteria (source: wikipedia)

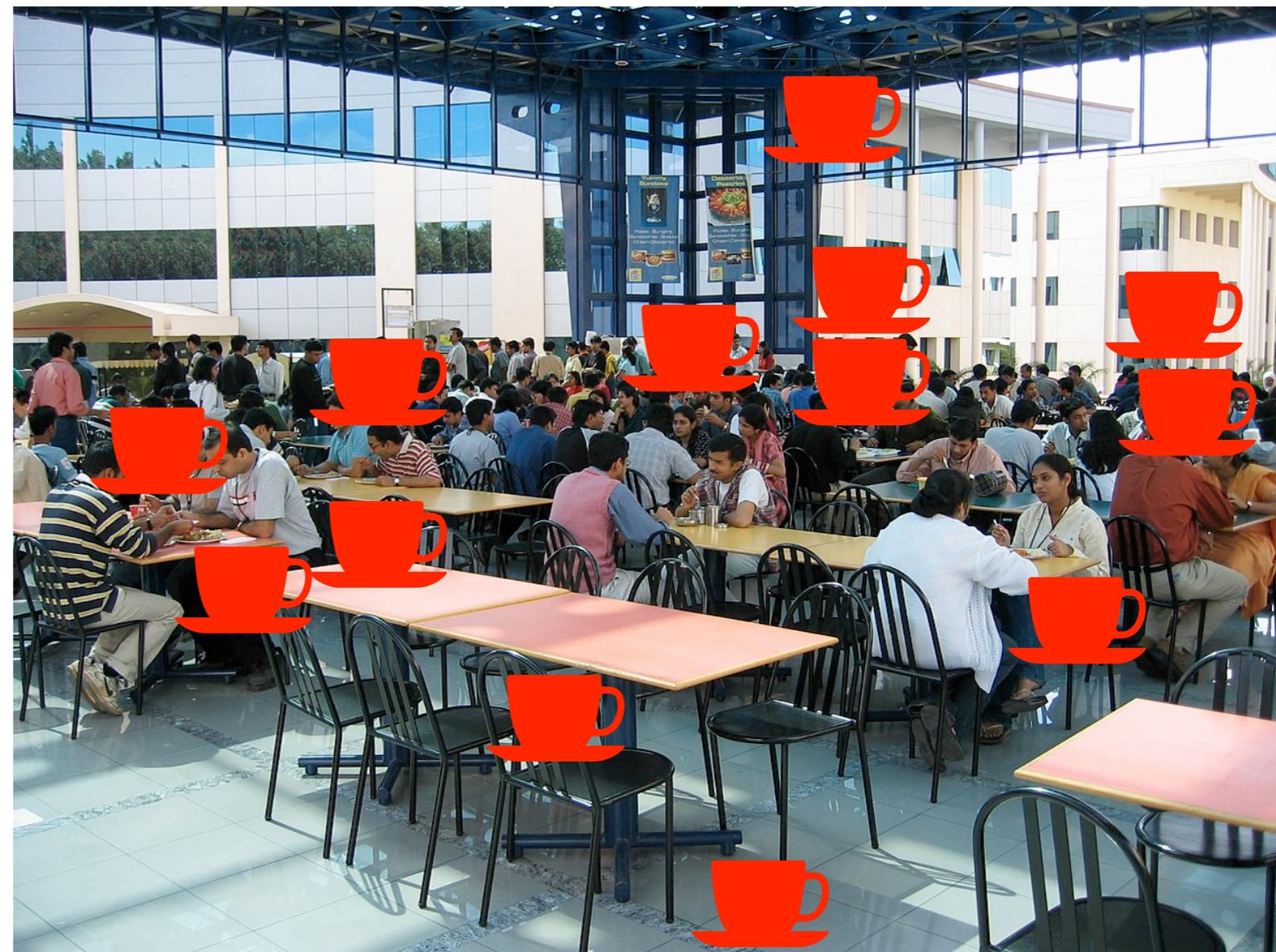
Evil coffee machines

Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems, David J. Agans, 2002



Around the same time, in the cafeteria...

During the 3pm coffee break, people started ordering coffees



Crowded cafeteria (source: wikipedia)

Evil coffee machines

Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems, David J. Agans, 2002



Around the same time, in the cafeteria...

During the 3pm coffee break, people started ordering coffees



Lots of coffees...



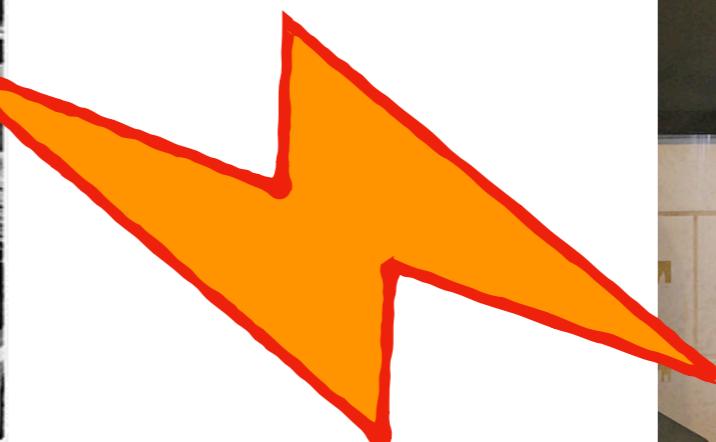
Crowded cafeteria (source: wikipedia)

Evil coffee machines

Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems, David J. Agans, 2002



Random bugs



Power drain



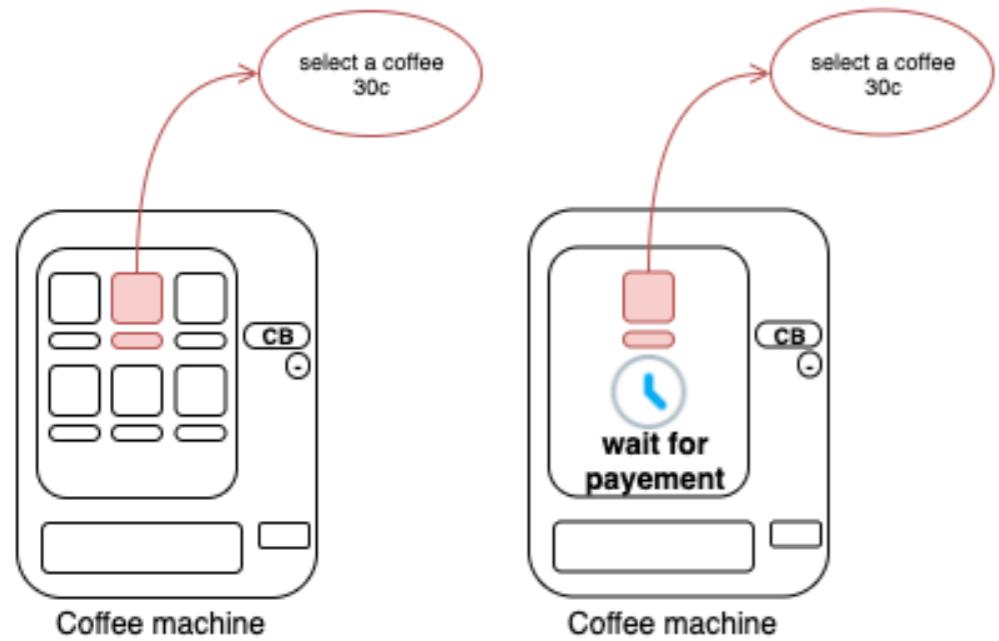
Coffee machines
(source: wikipedia)

From real experience.

The coffee machines timeout at Univ. Lille

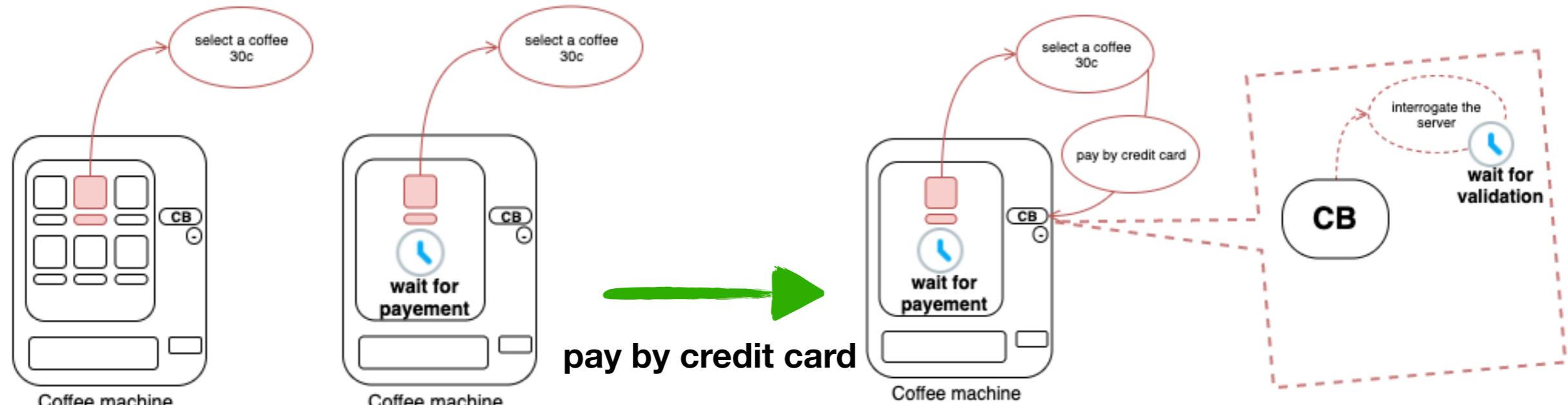
(you can even try it!)

The coffee machines timeout at Univ. Lille



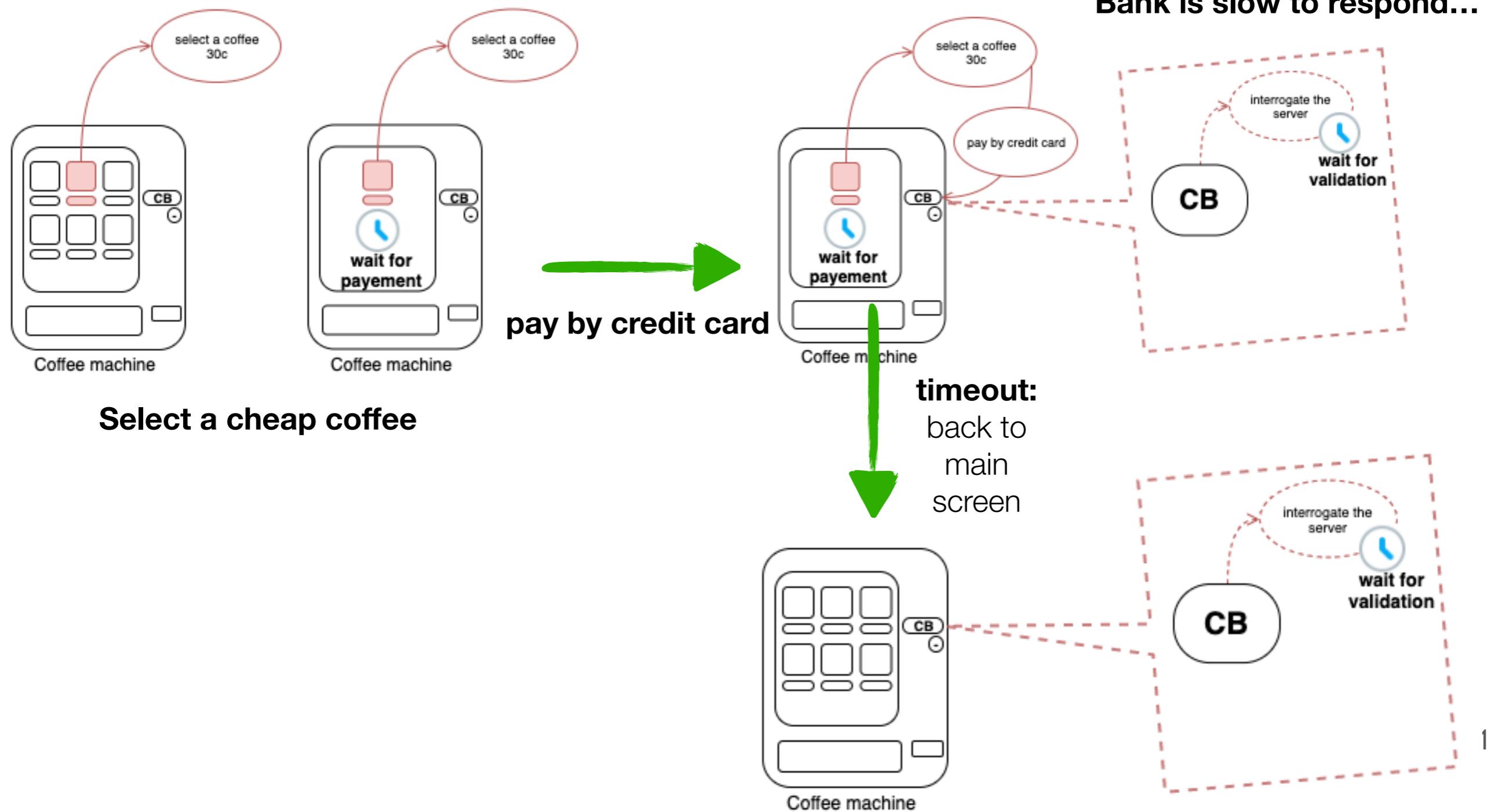
Select a cheap coffee

The coffee machines timeout at Univ. Lille

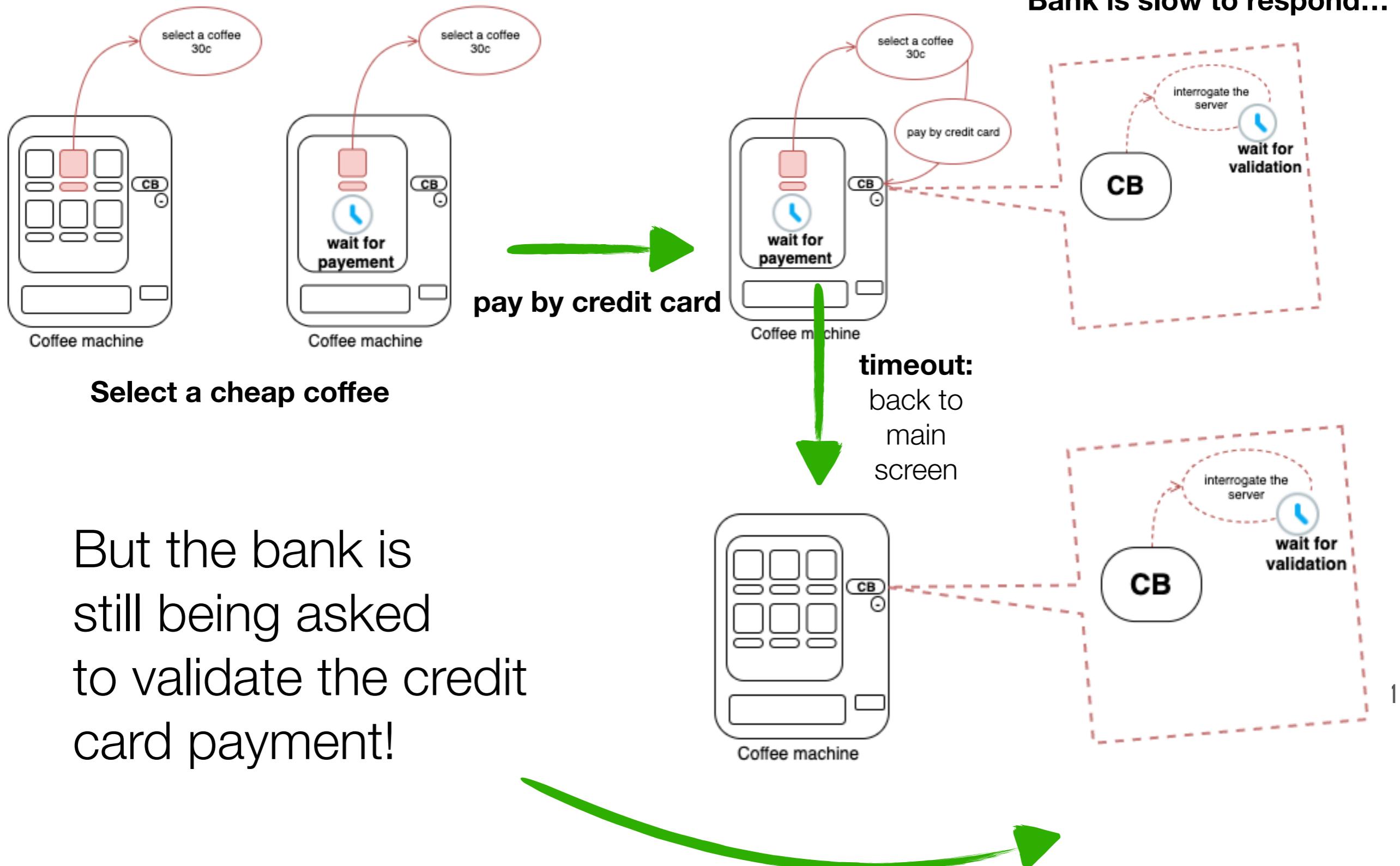


Select a cheap coffee

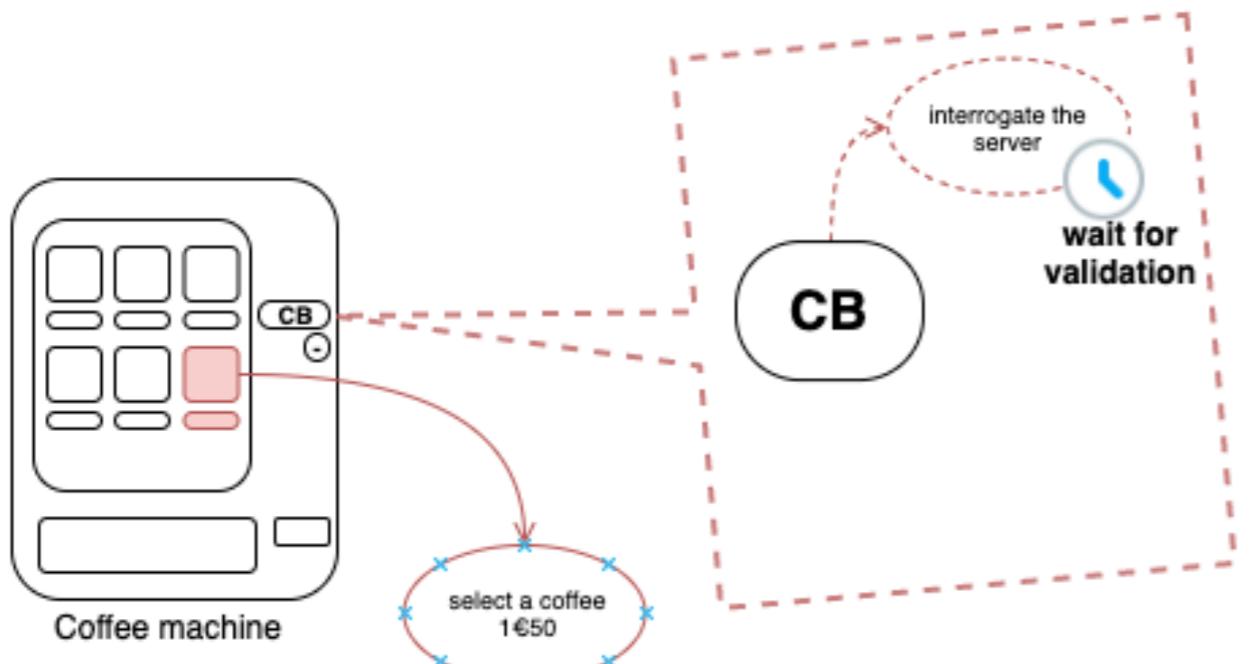
The coffee machines timeout at Univ. Lille



The coffee machines timeout at Univ. Lille

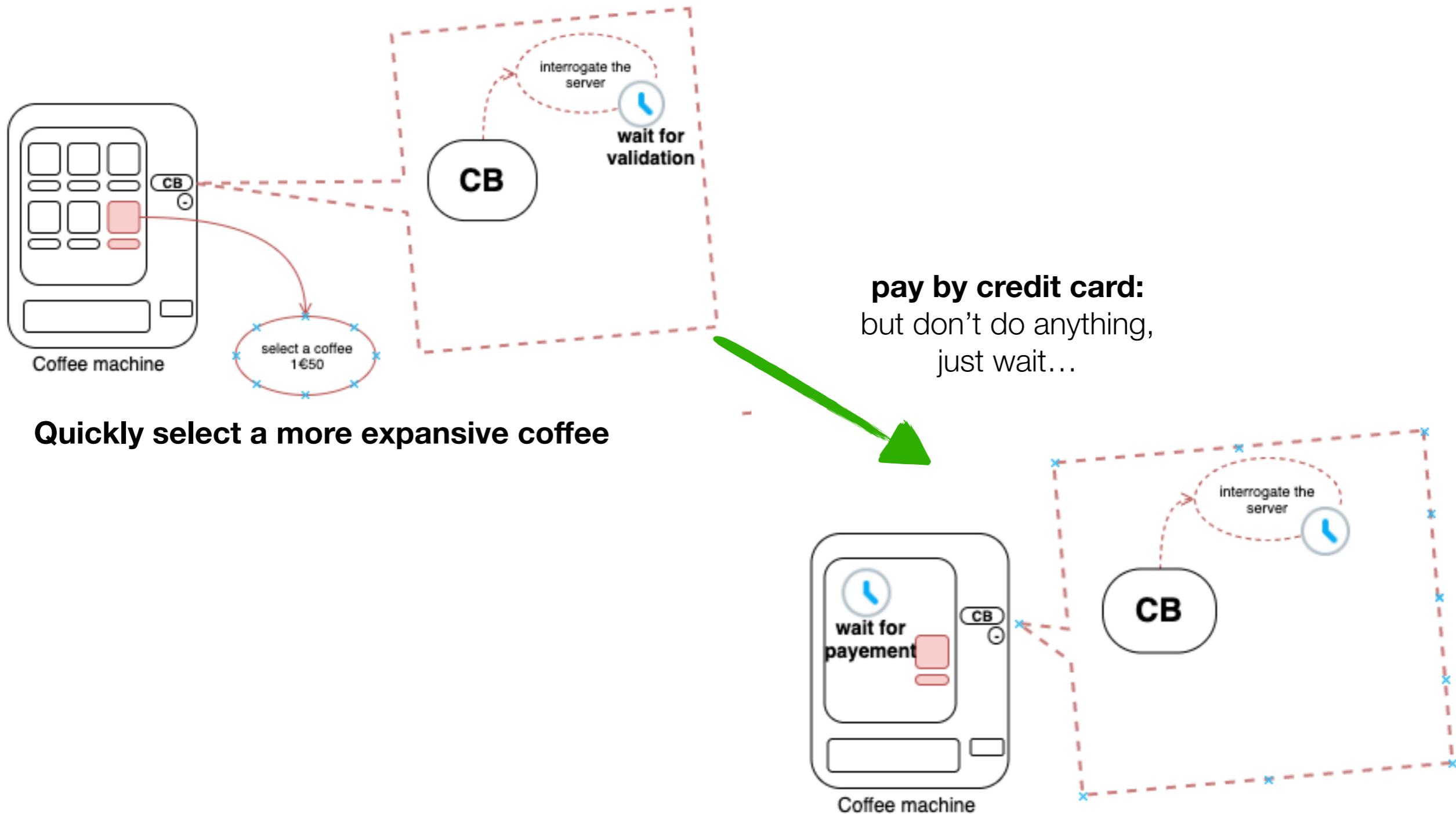


The coffee machines timeout at Univ. Lille

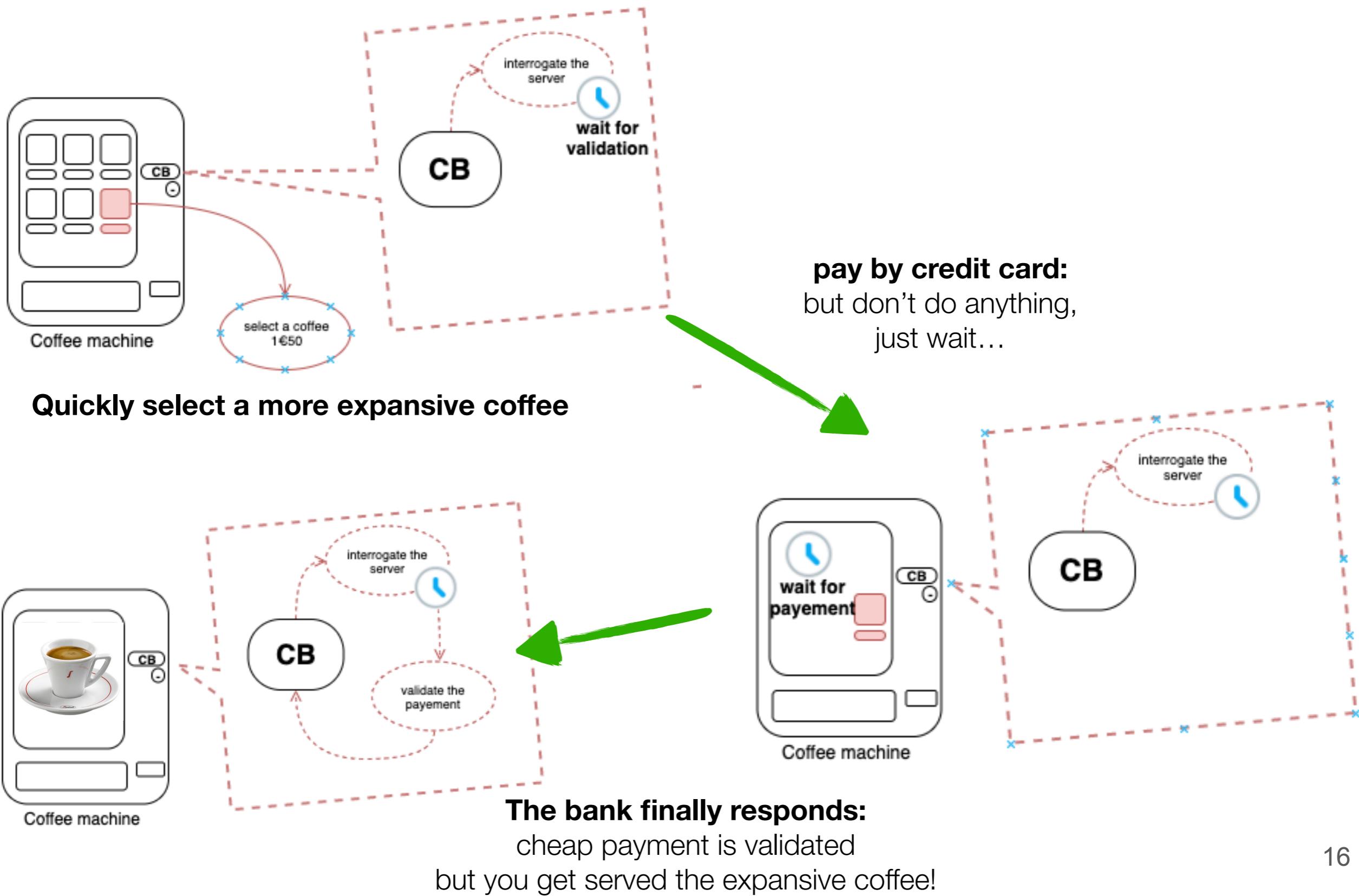


Quickly select a more expansive coffee

The coffee machines timeout at Univ. Lille



The coffee machines timeout at Univ. Lille



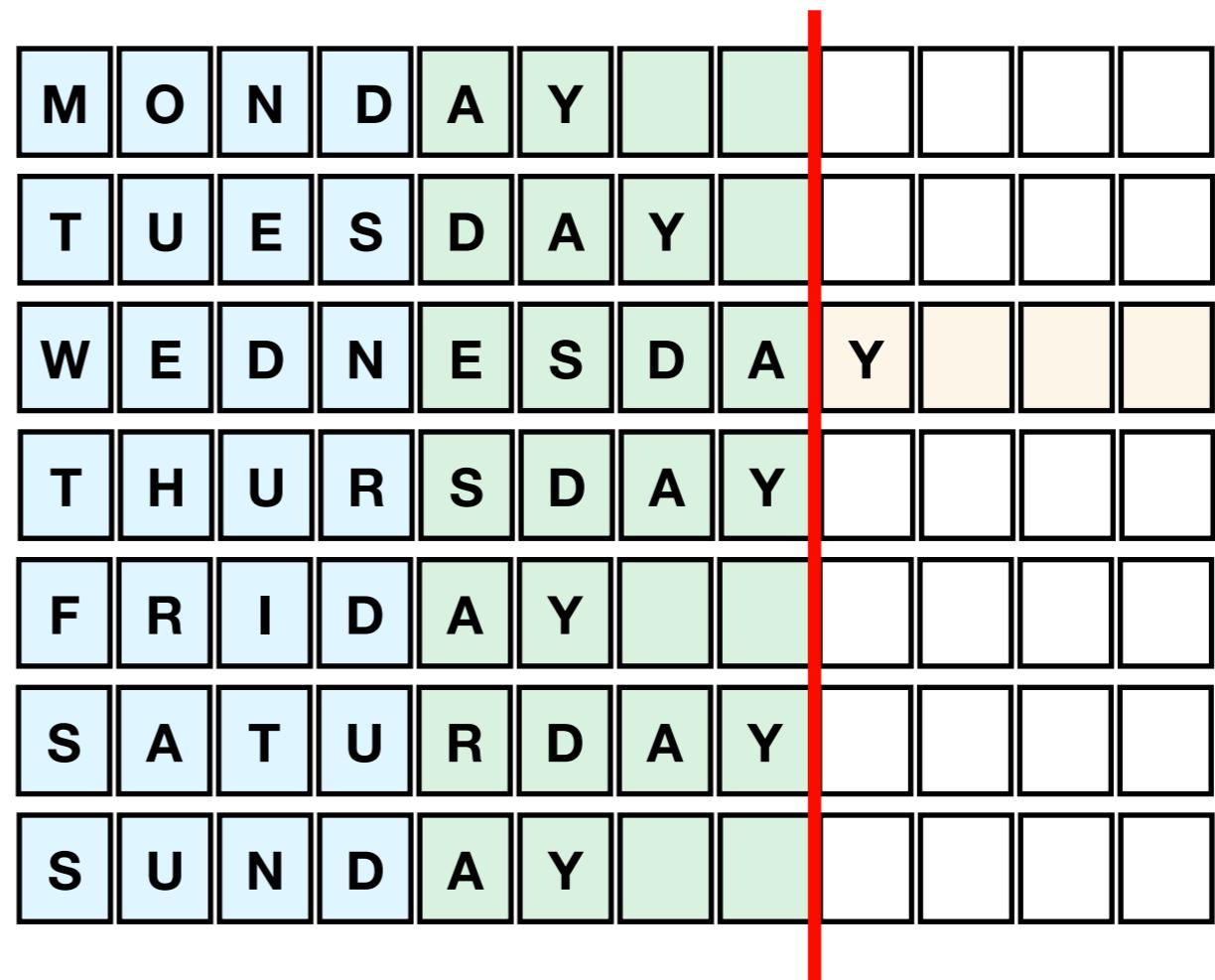
Only wednesdays

My Hairiest Bug War Stories,
Mark Eisenstadt, 1997 (Story B)

Only Wednesdays

My Hairiest Bug War Stories,
Mark Eisenstadt, 1997

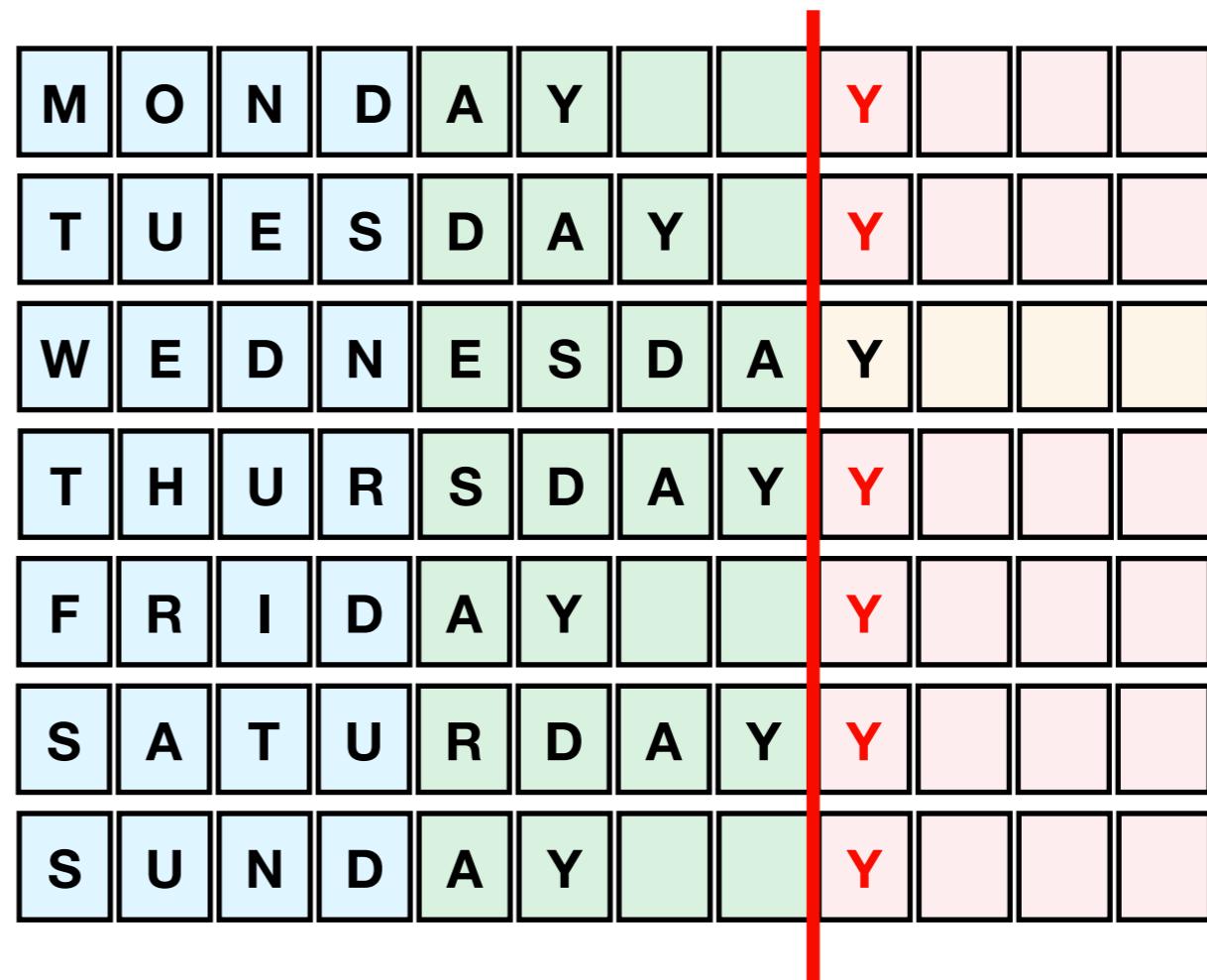
- A program was only working properly on wednesdays...
- **Documentation stated that day of the week was returned in a doubleword — 8 bytes**
 - But as Wednesday is 9 characters long, the system was expecting a three words array — 12 bytes
 - For the six other days of the week, the additional 4 bytes were programmatically filled out with blanks, as only 8 bytes were necessary



Only Wednesdays

My Hairiest Bug War Stories,
Mark Eisenstadt, 1997

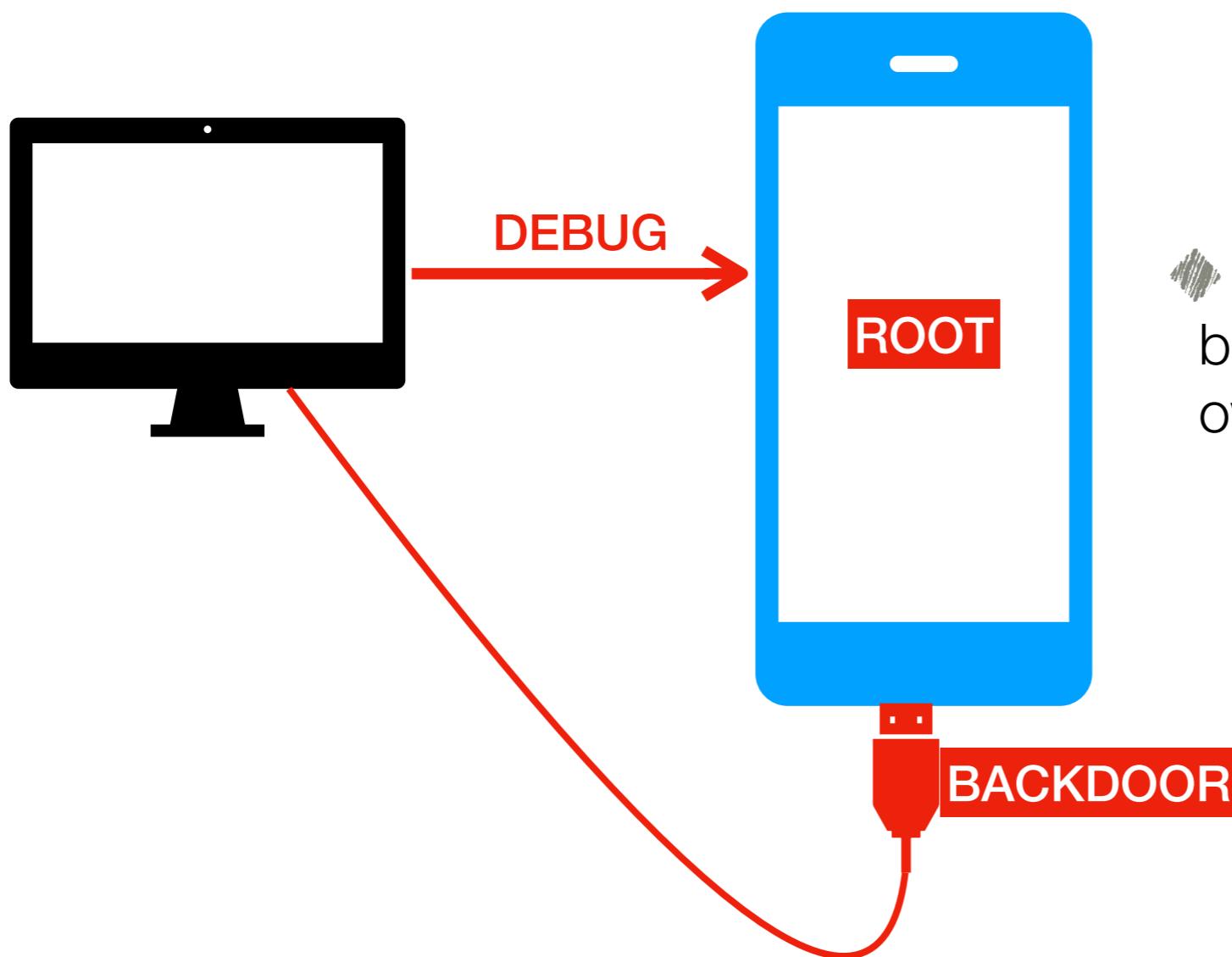
- A program was only working properly on wednesdays...
- **Documentation stated that day of the week was returned in a doubleword — 8 bytes**
 - But as Wednesday is 9 characters long, the system was expecting a three words array — 12 bytes
 - For the six other days of the week, the additional 4 bytes were programmatically filled out with blanks, as only 8 bytes were necessary
- **Unfortunately, those 4 additional bytes were also used to store another character «y», to compare with users' answers (« yes » or « no »)**
 - This value was wiped out 6 days out of 7
 - On Wednesdays, the value was stored in its correct place because it is the last character of «Wednesday»



The Android « root-console » problem

The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009

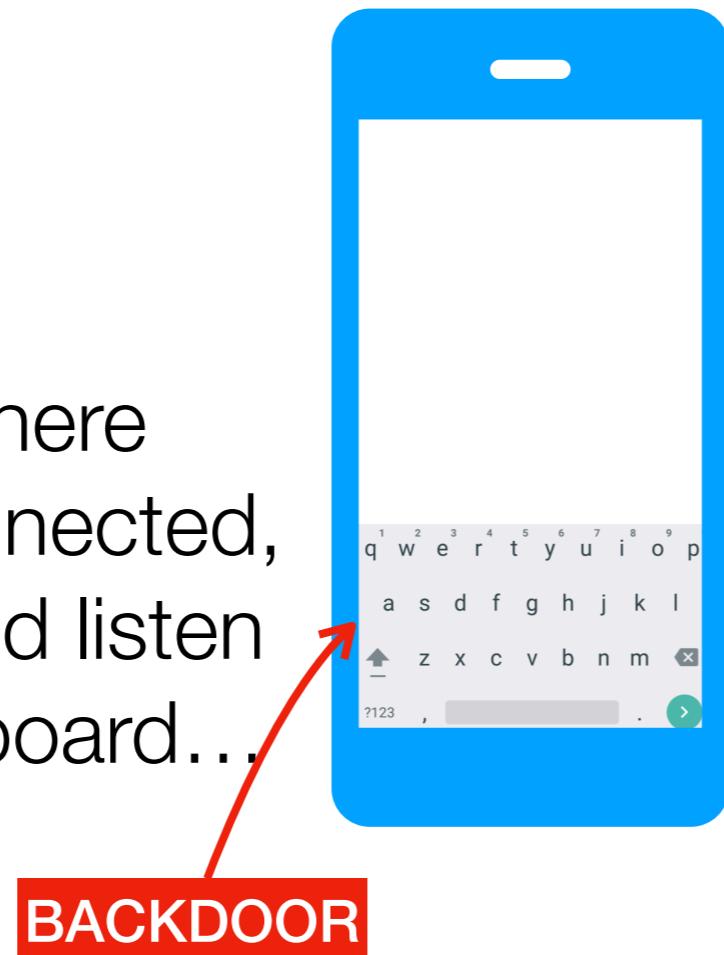


- ◆ Google engineers implemented a backdoor to connect remote devices over the serial port for debugging

The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009

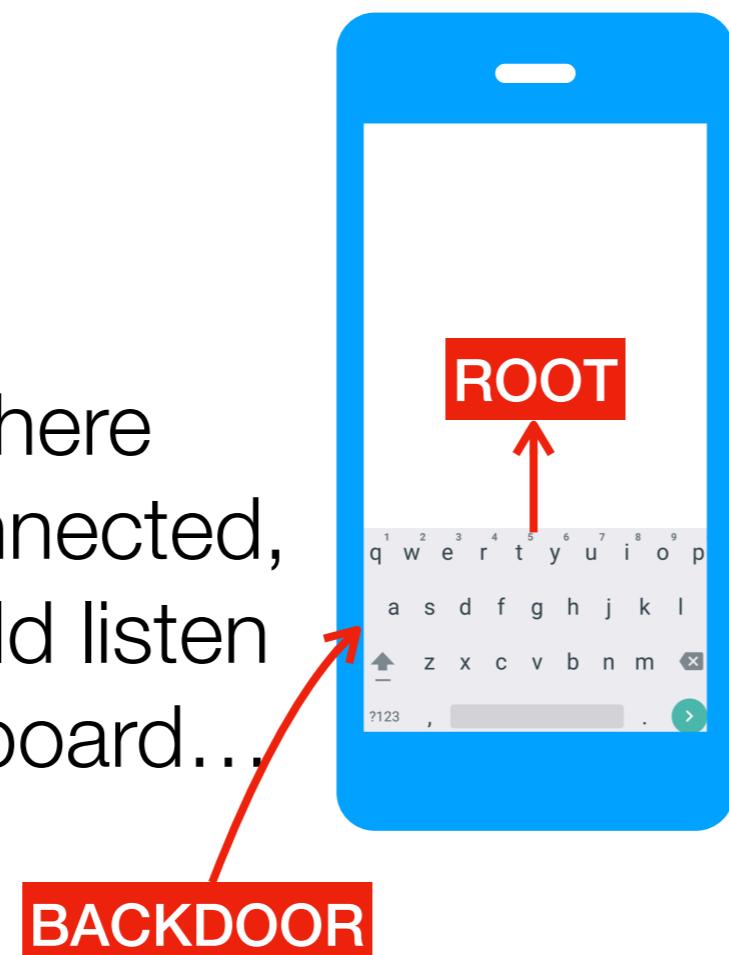
- However, when there was no device connected, the backdoor would listen to the system keyboard...



The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009

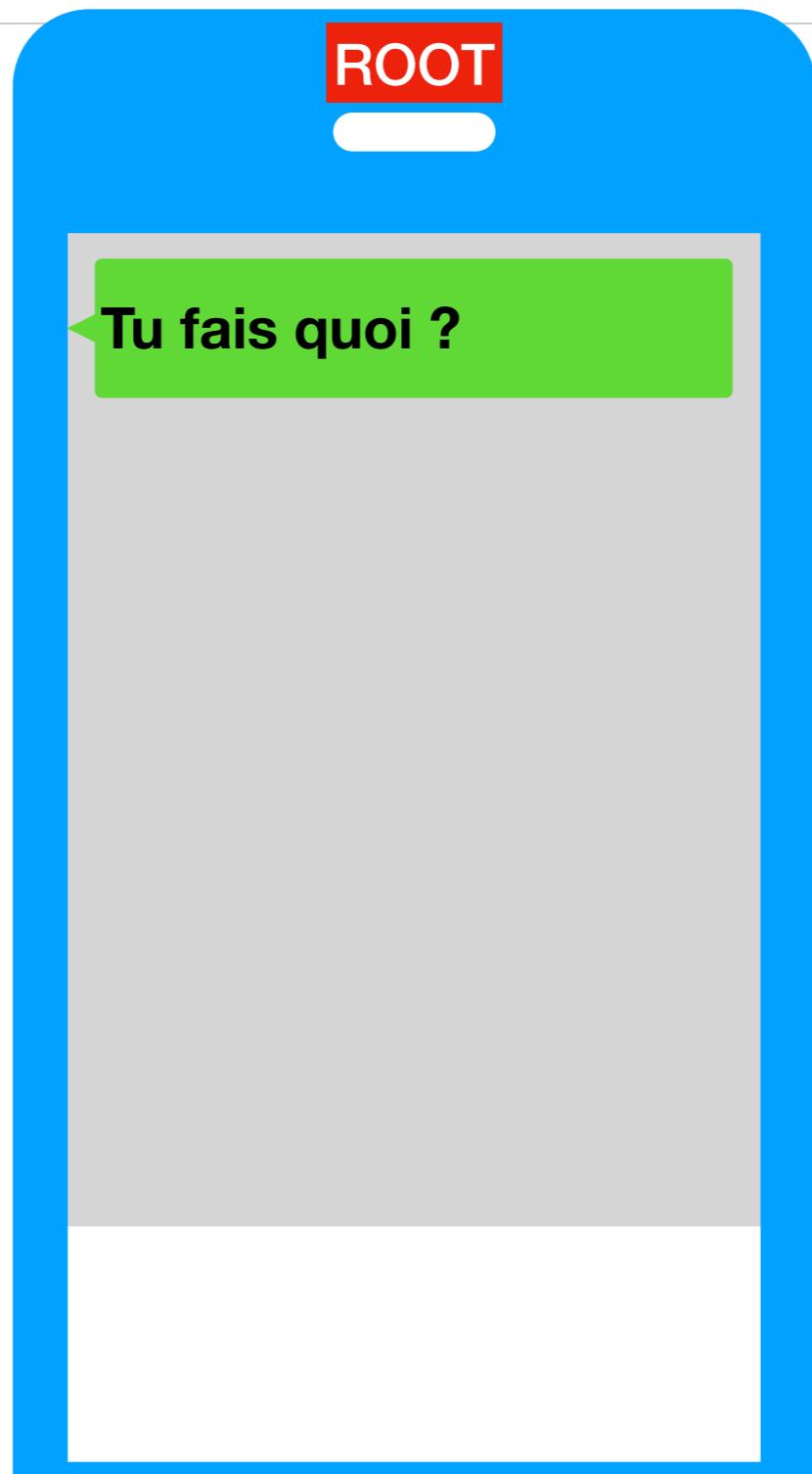
- However, when there was no device connected, the backdoor would listen to the system keyboard...



Any text that people typed was then executed as a command with superuser privileges...

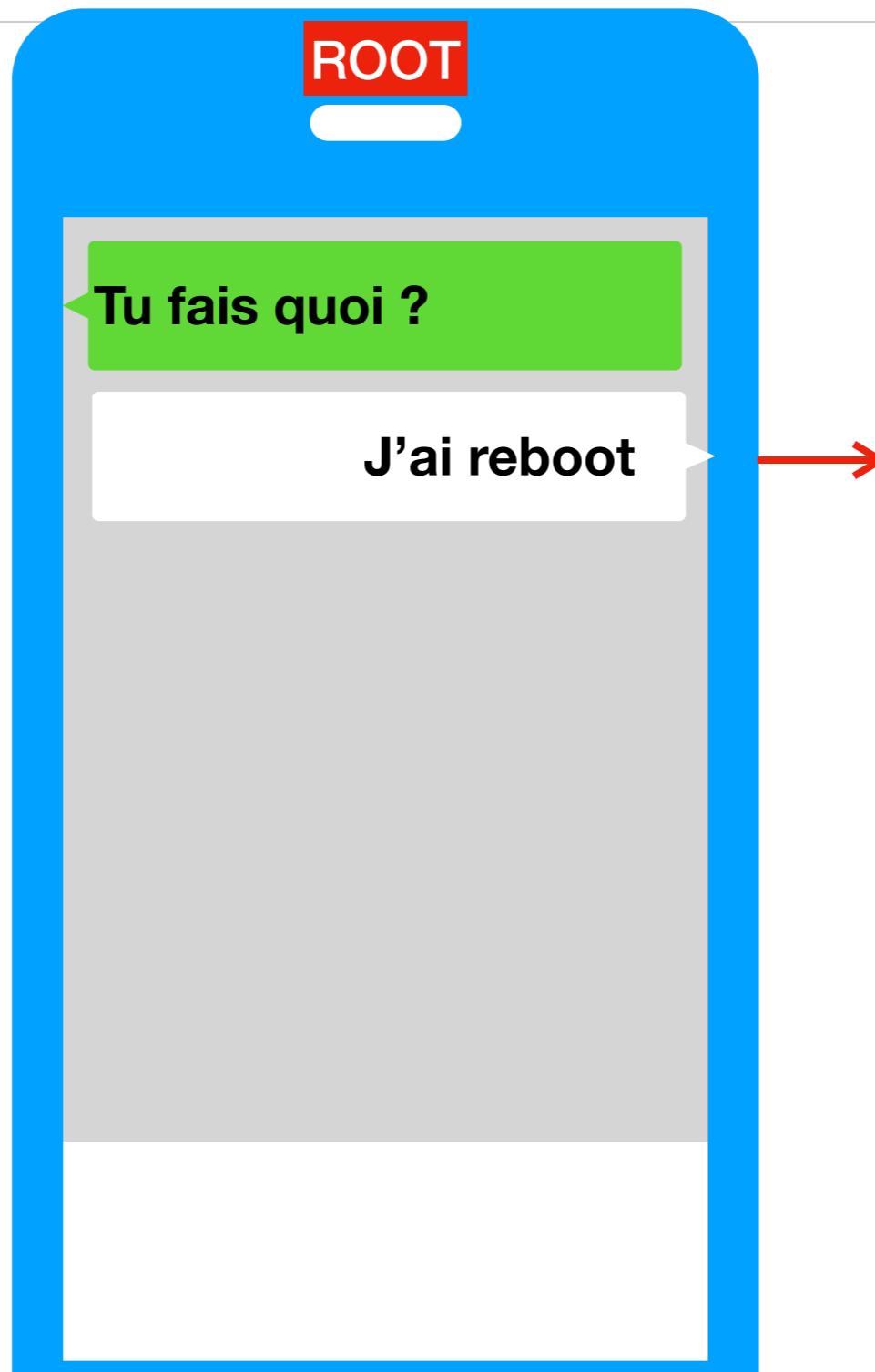
The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009



The Android « root-console » bug

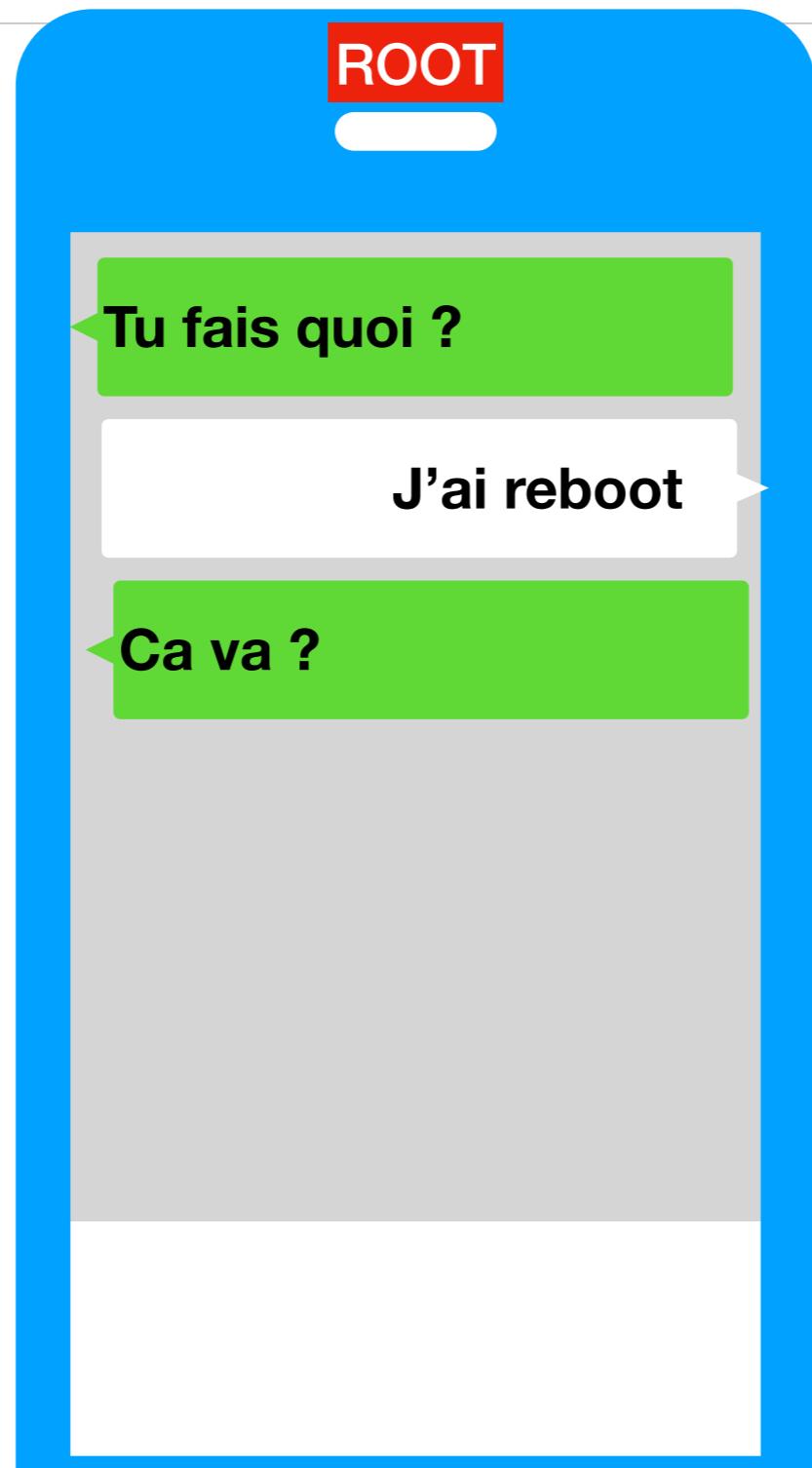
Why Programs Fail, Andreas Zeller, 2009



Redémarre le
téléphone

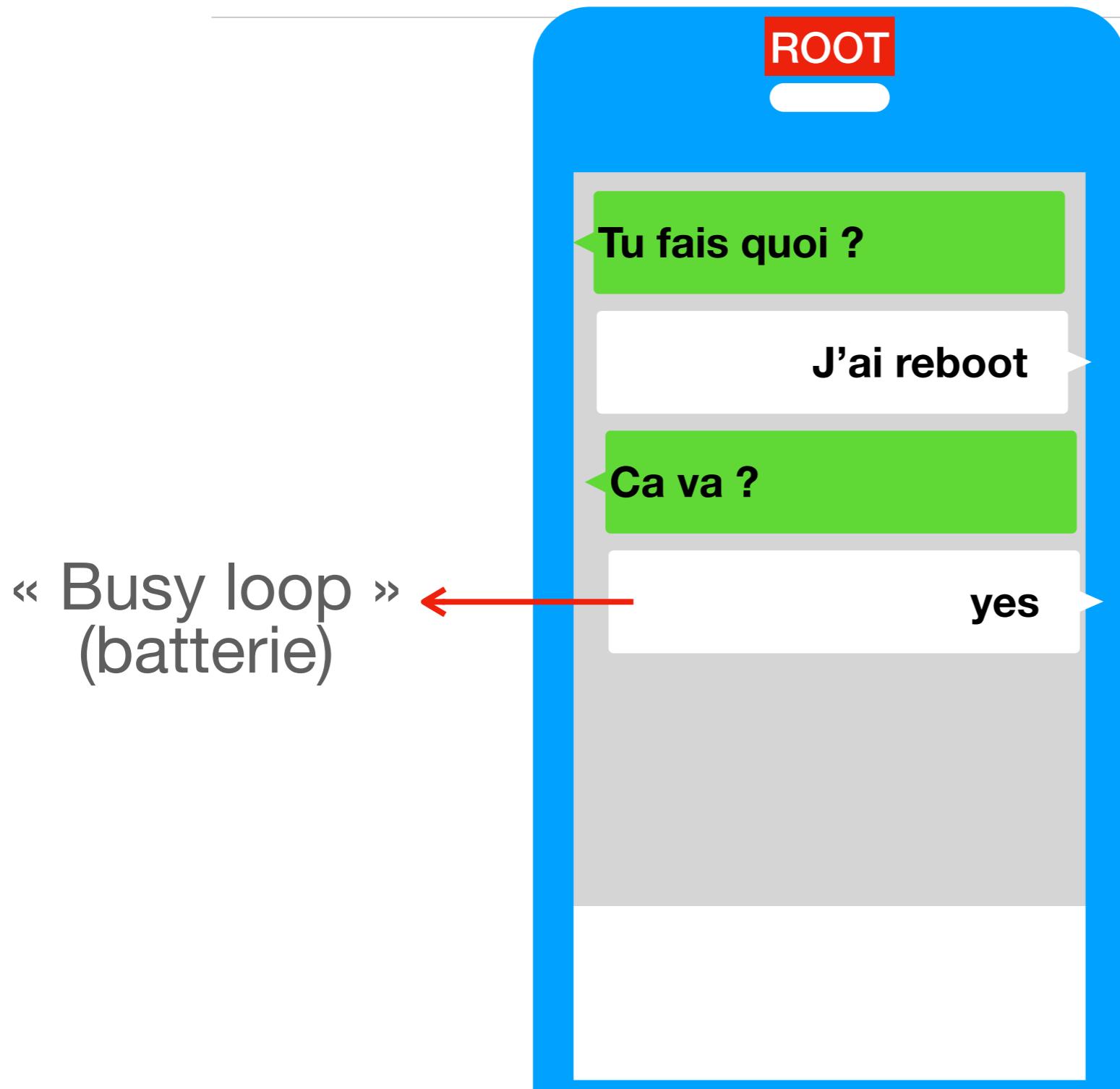
The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009



The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009



The Android « root-console » bug

Why Programs Fail, Andreas Zeller, 2009



The Android « root-console » bug

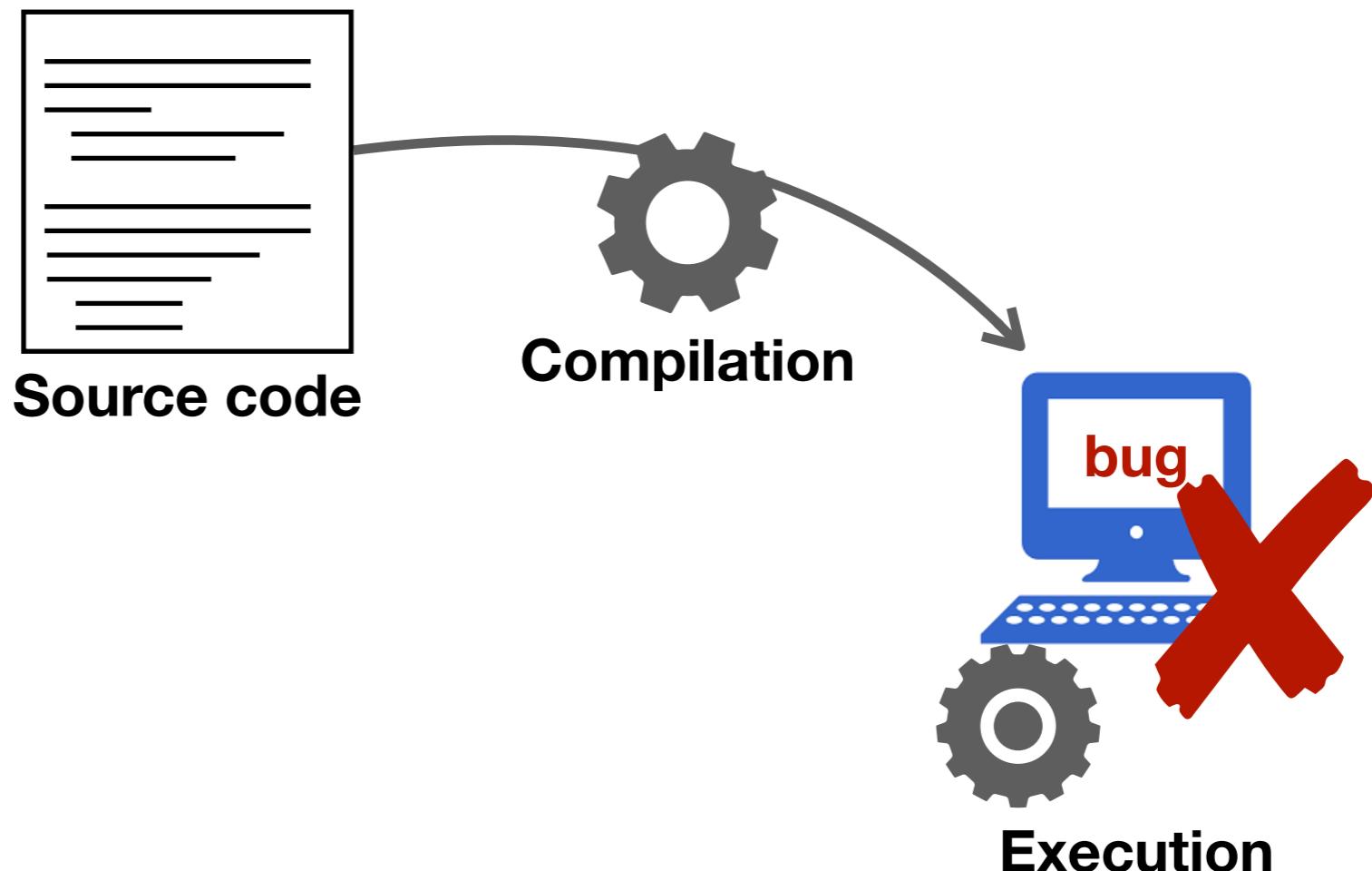
Why Programs Fail, Andreas Zeller, 2009



Tool interference

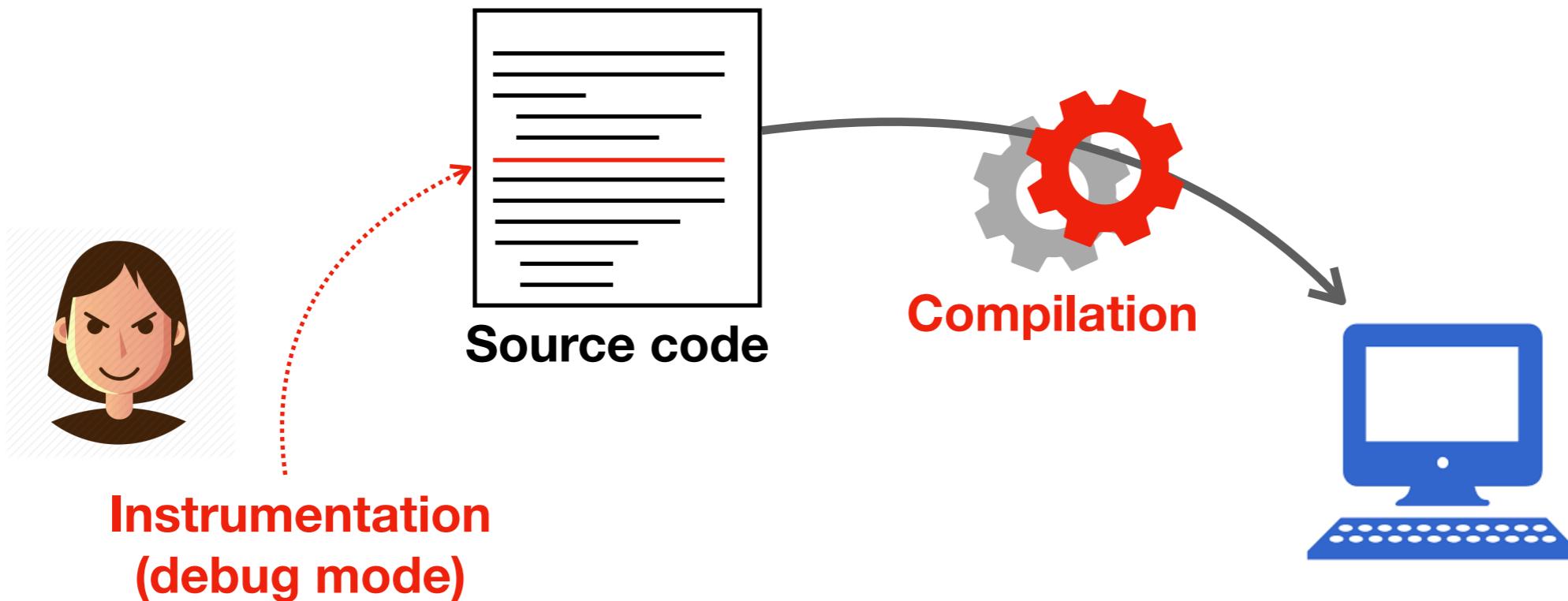
Tool interference

Why Programs Fail, Andreas Zeller, 2009



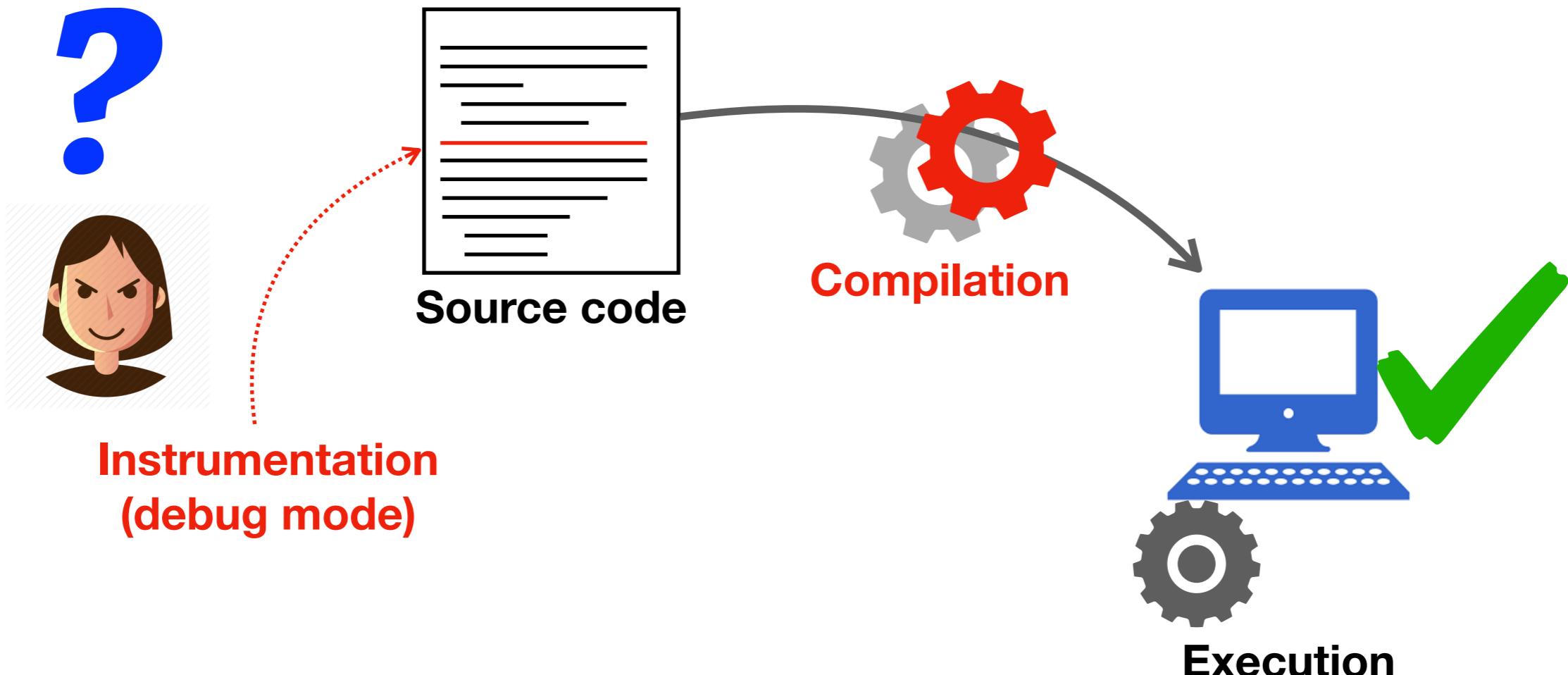
Tool interference

Why Programs Fail, Andreas Zeller, 2009



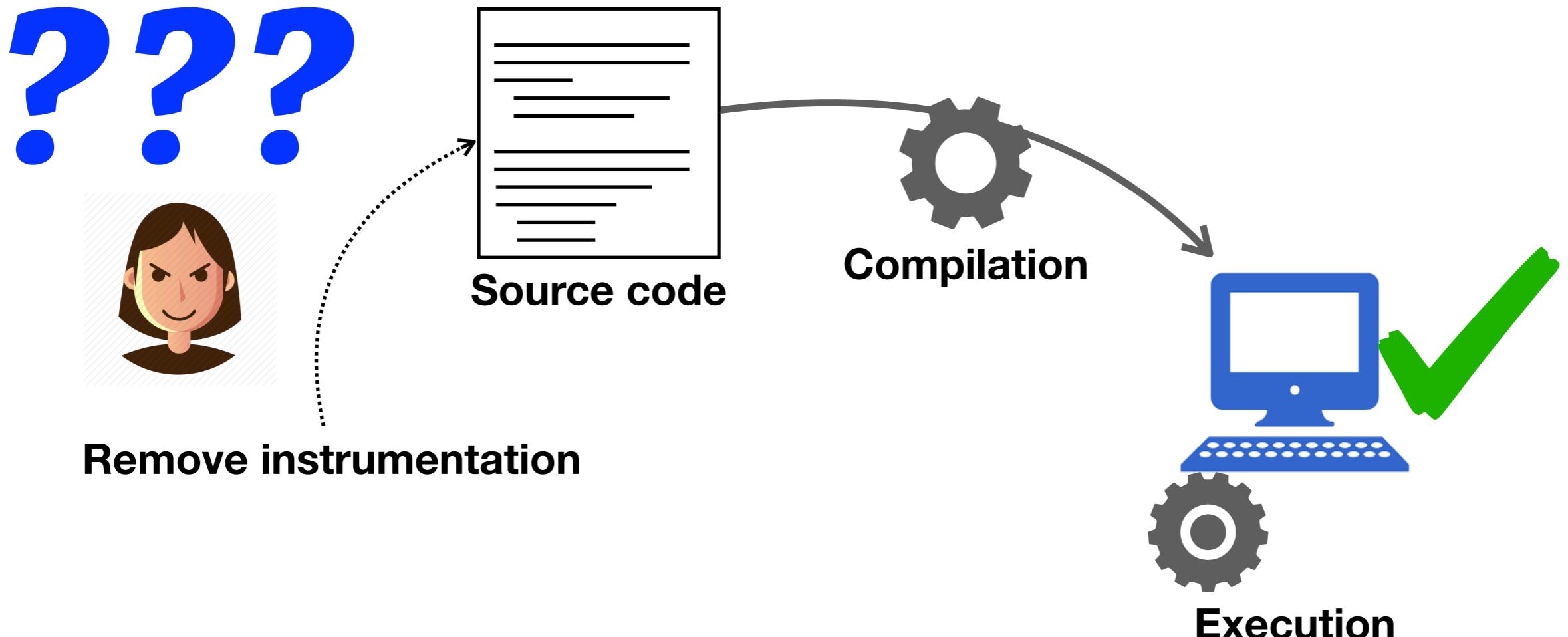
Tool interference

Why Programs Fail, Andreas Zeller, 2009



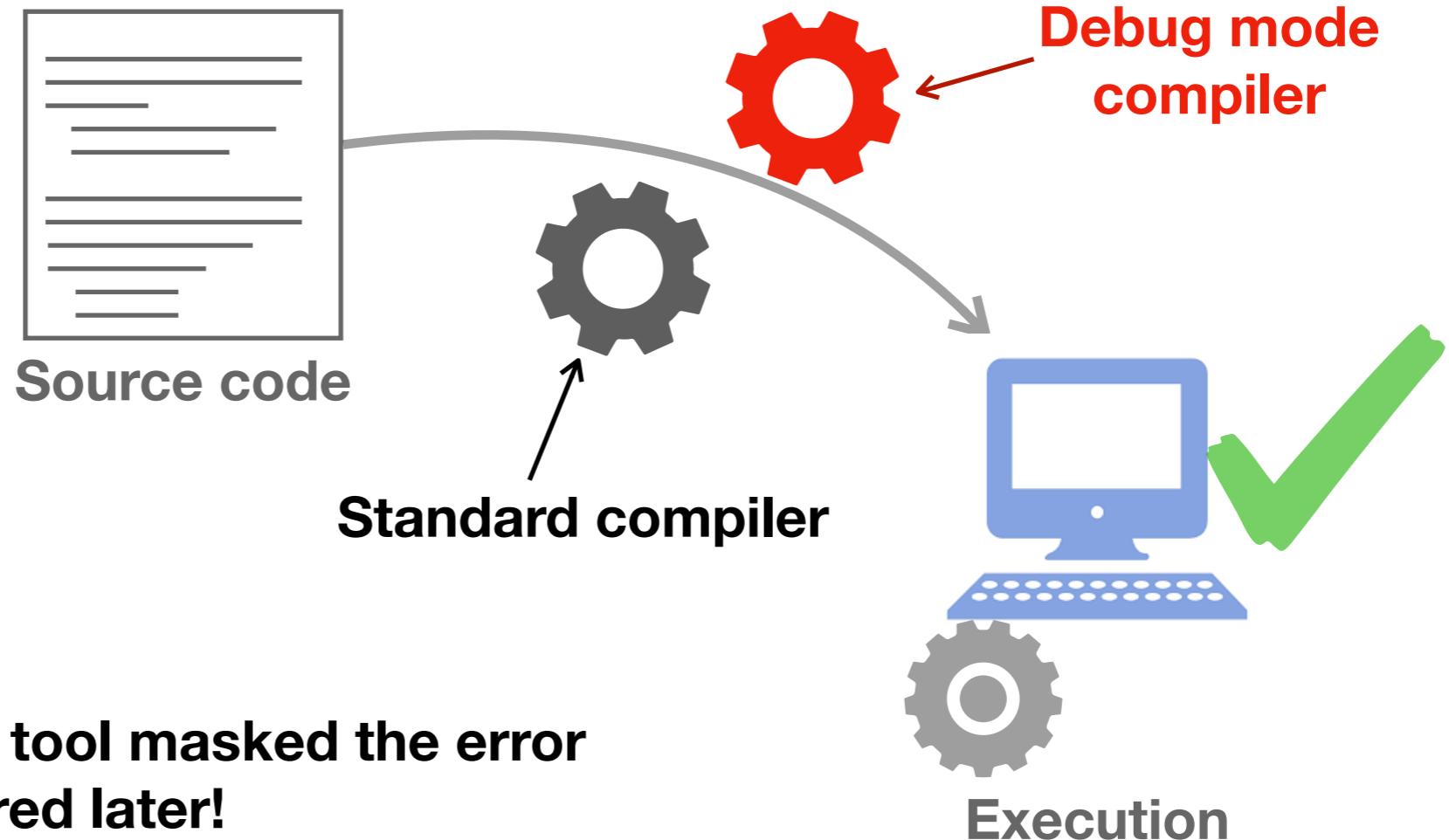
Tool interference

Why Programs Fail, Andreas Zeller, 2009



Tool interference

Why Programs Fail, Andreas Zeller, 2009

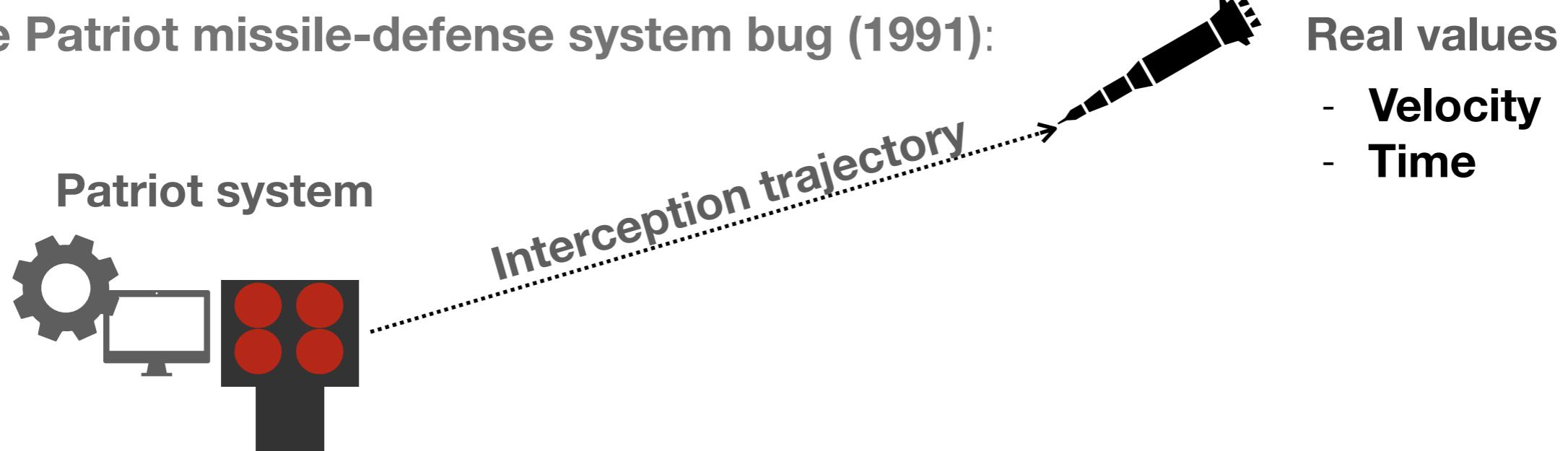


The patriot interception system bug

Fighting bugs: Remove, retry, replicate,
and rejuvenate, Grotte and Trivedi, 2007

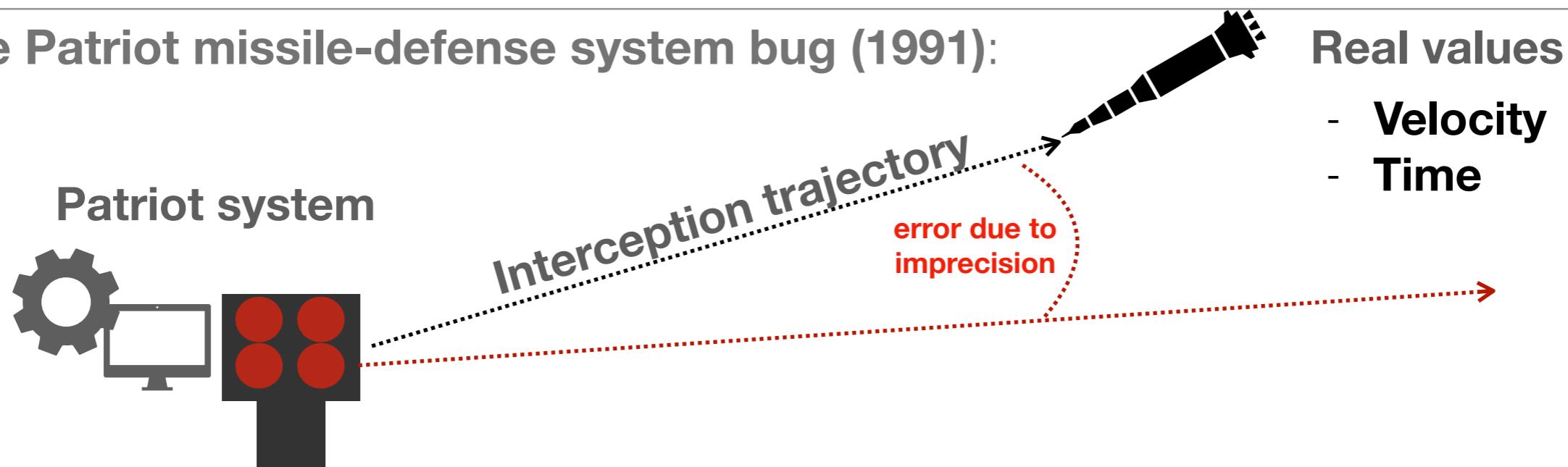
The patriot interception system bug

The Patriot missile-defense system bug (1991):



The patriot interception system bug

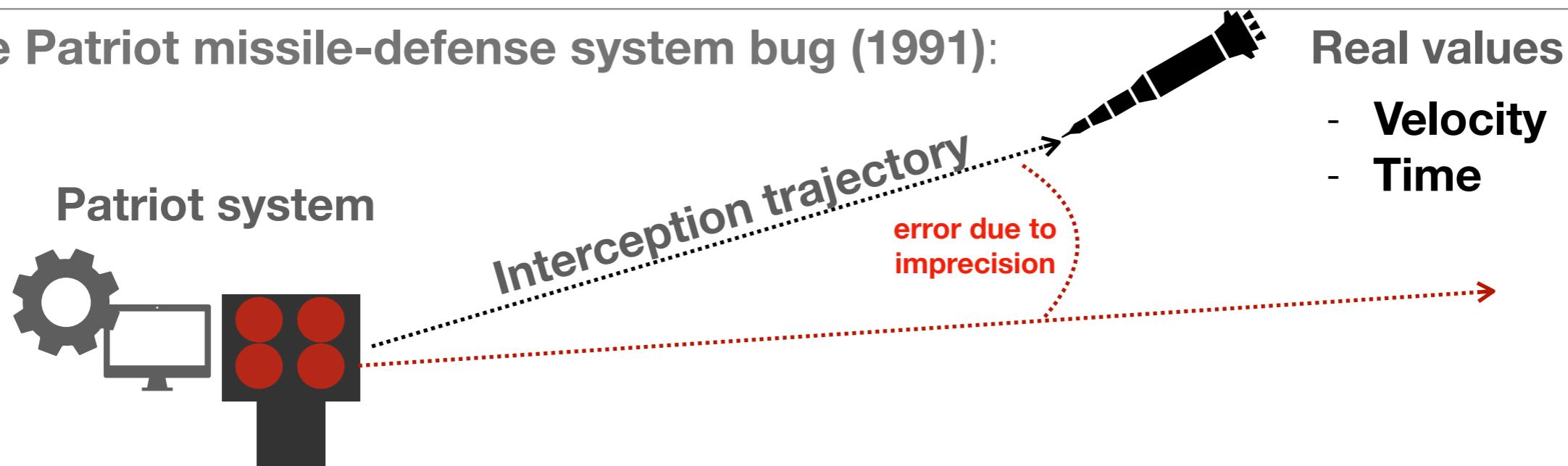
The Patriot missile-defense system bug (1991):



- Time internally represented as an integer!
- Conversion to a real value was imprecise
- Imprecision augmented with time!

The patriot interception system bug

The Patriot missile-defense system bug (1991):



- Time internally represented as an integer!
- Conversion to a real value was imprecise
- Imprecision augmented with time!

1991, Dharhan, Saudi Arabia: after 20 hours of run time, the system missed an interception because of this bug (28 dead, 97 wounded)

The Therac-25 bugs

The Science of Debugging, Telles and Hsieh, 2001

The Therac-25 bug (one of them...)

Radiation therapy machine used in the 80's

Entirely controlled by software



**Bugs:
radiation overdose of 6 patients, 3 died**

The Science of Debugging, Telles and Hsieh, 2001

The Therac-25 bug (one of them...)

Error counter:
0 = SAFE



The Science of Debugging, Telles and Hsieh, 2001

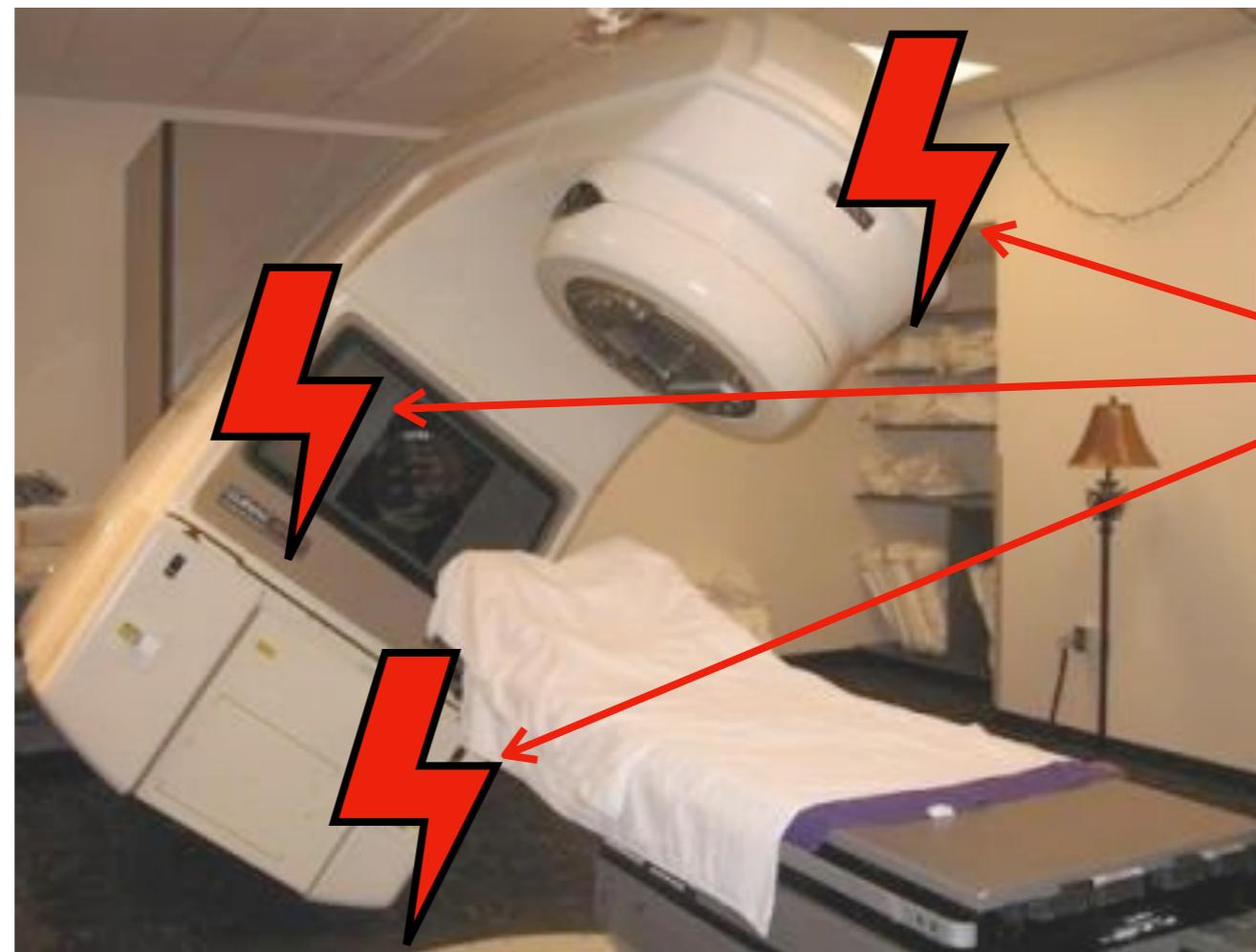
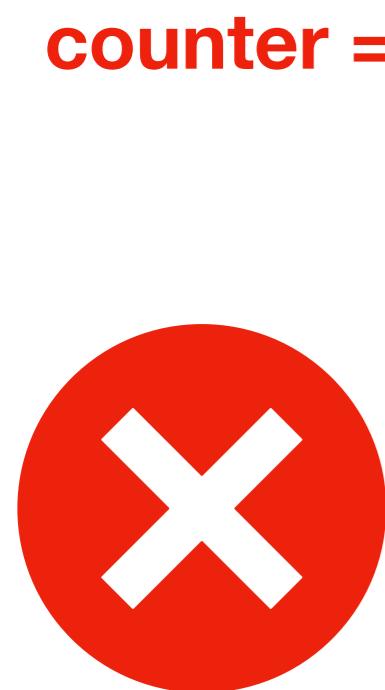
The Therac-25 bug (one of them...)

Error counter:

>0 = DANGER



The Therac-25 bug (one of them...)



The Therac-25 bug (one of them...)



counter = 75



The Science of Debugging, Telles and Hsieh, 2001

The Therac-25 bug (one of them...)



counter = 197



The Science of Debugging, Telles and Hsieh, 2001

The Therac-25 bug (one of them...)



counter = 255



The Science of Debugging, Telles and Hsieh, 2001

The Therac-25 bug (one of them...)

counter = 0



The Science of Debugging, Telles and Hsieh, 2001

The Therac-25 bug (one of them...)

**Counter variable
encoded on one
byte!**

counter = 0



The Therac-25 bug (one of them...)

Counter variable encoded on one byte!



counter = 0



Pressing « start »:
if done at the precise
« rollover » moment,
delivers the full
radiation dose to the
patient!

Bibliography

References

- 1.<https://www.ibiblio.org/harris/500milemail.html>
- 2.**Debugging: The 9 indispensable rules for finding even the most elusive software and hardware problems**, David J. Agans, 2002
- 3.**Why Programs Fail**, Andreas Zeller, 2009
- 4.**My Hairiest Bug War Stories**, Mark Eisenstadt, 1997
- 5.**Fighting bugs: Remove, retry, replicate, and rejuvenate**, Grotte and Trivedi, 2007
- 6.**The Science of Debugging**, Telles and Hsieh, 2001