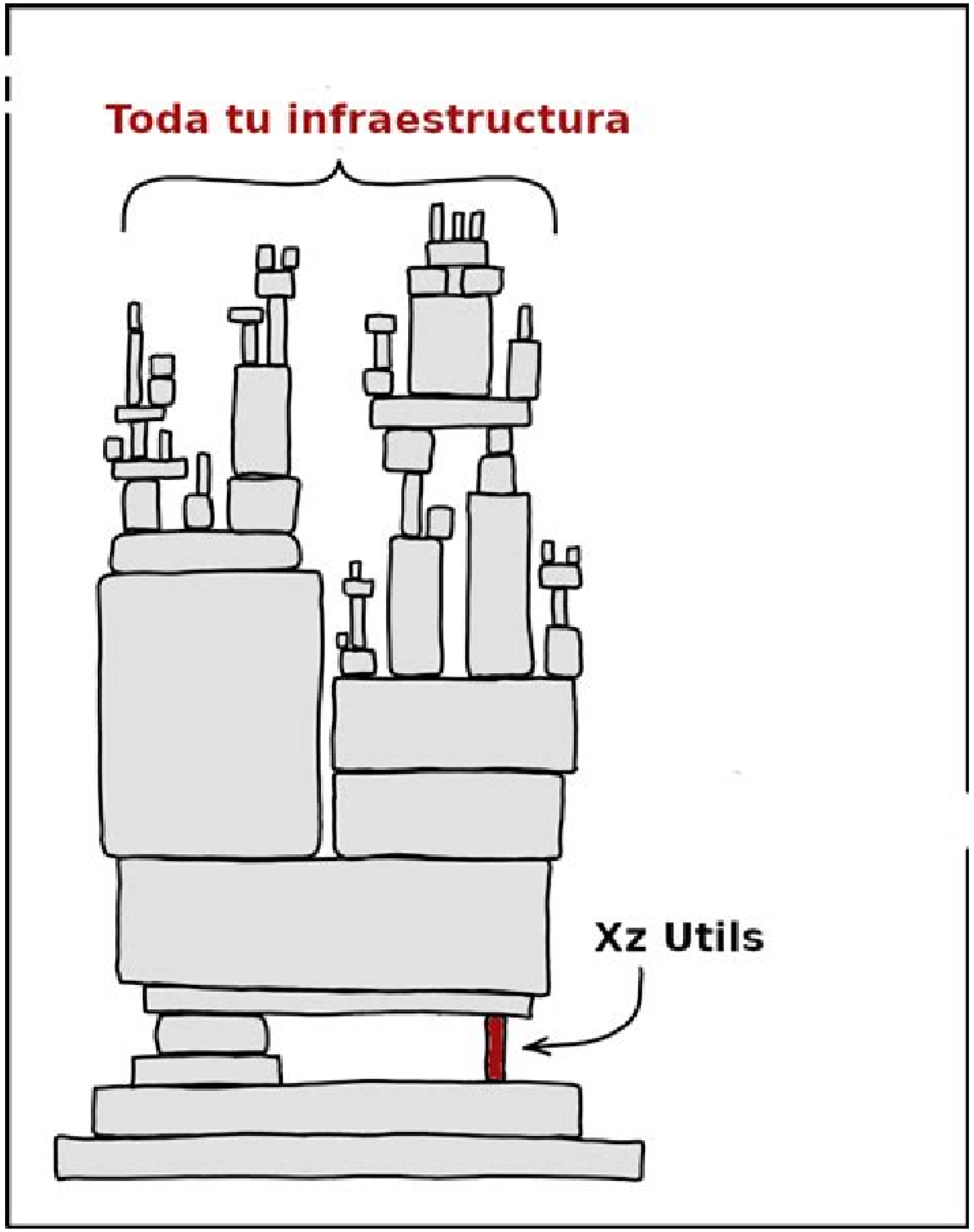
XZ utils infiltration (2024)

At some day someone noticed that SSH was 500ms slower and a chain of events followed

This software supply chain attack would almost comprimse all linux boxes

A Stuxnet level infiltration

So, what is XZ


Toda tu infraestructura
Xz Utils

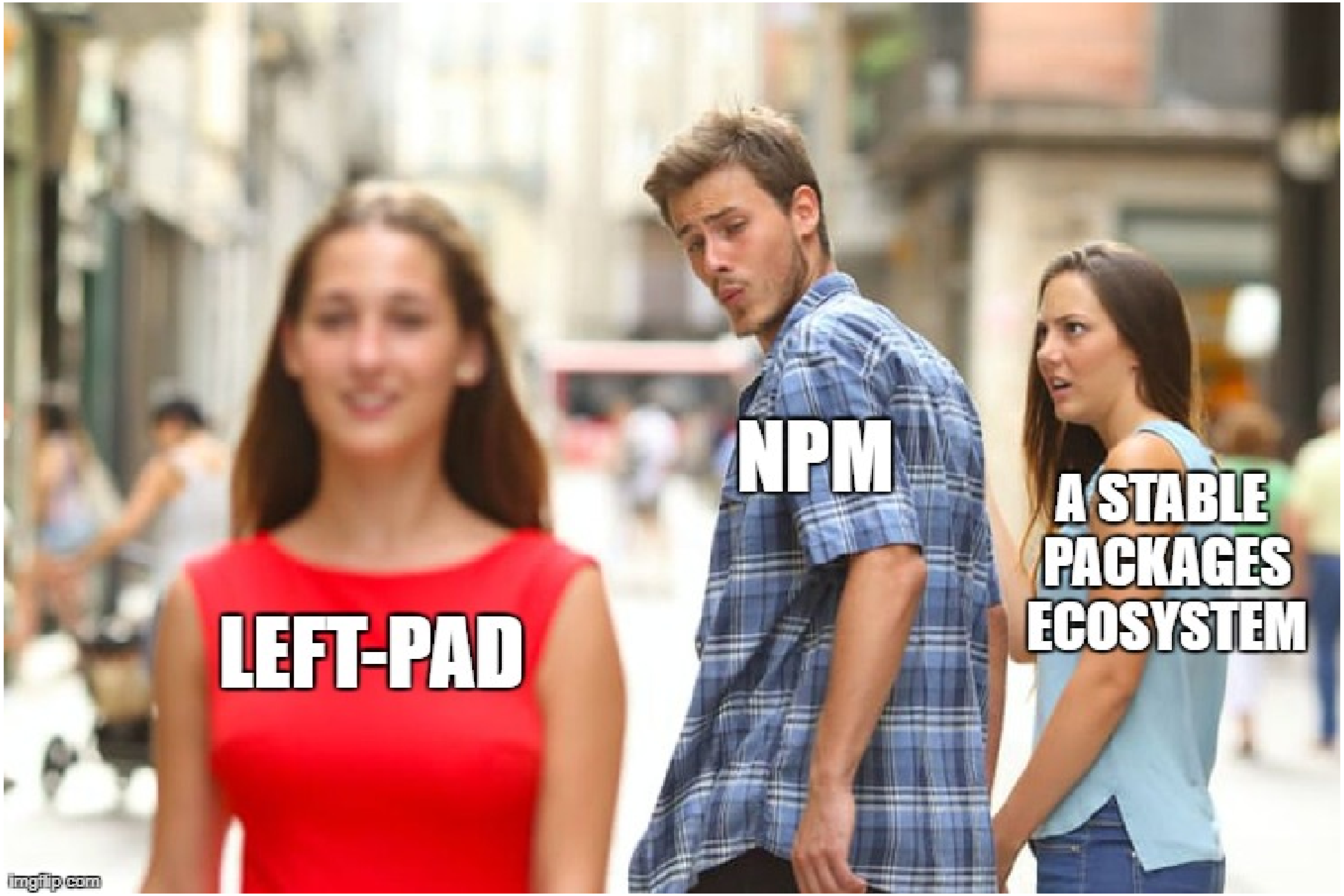
So, what is a supply chain attack

Supply chain attack is recent attack vector, getting more common

Just this week npm package "isarray" (yes you read that correctly) got compromised

With larger deps stack and neglected open source package more attack vectors

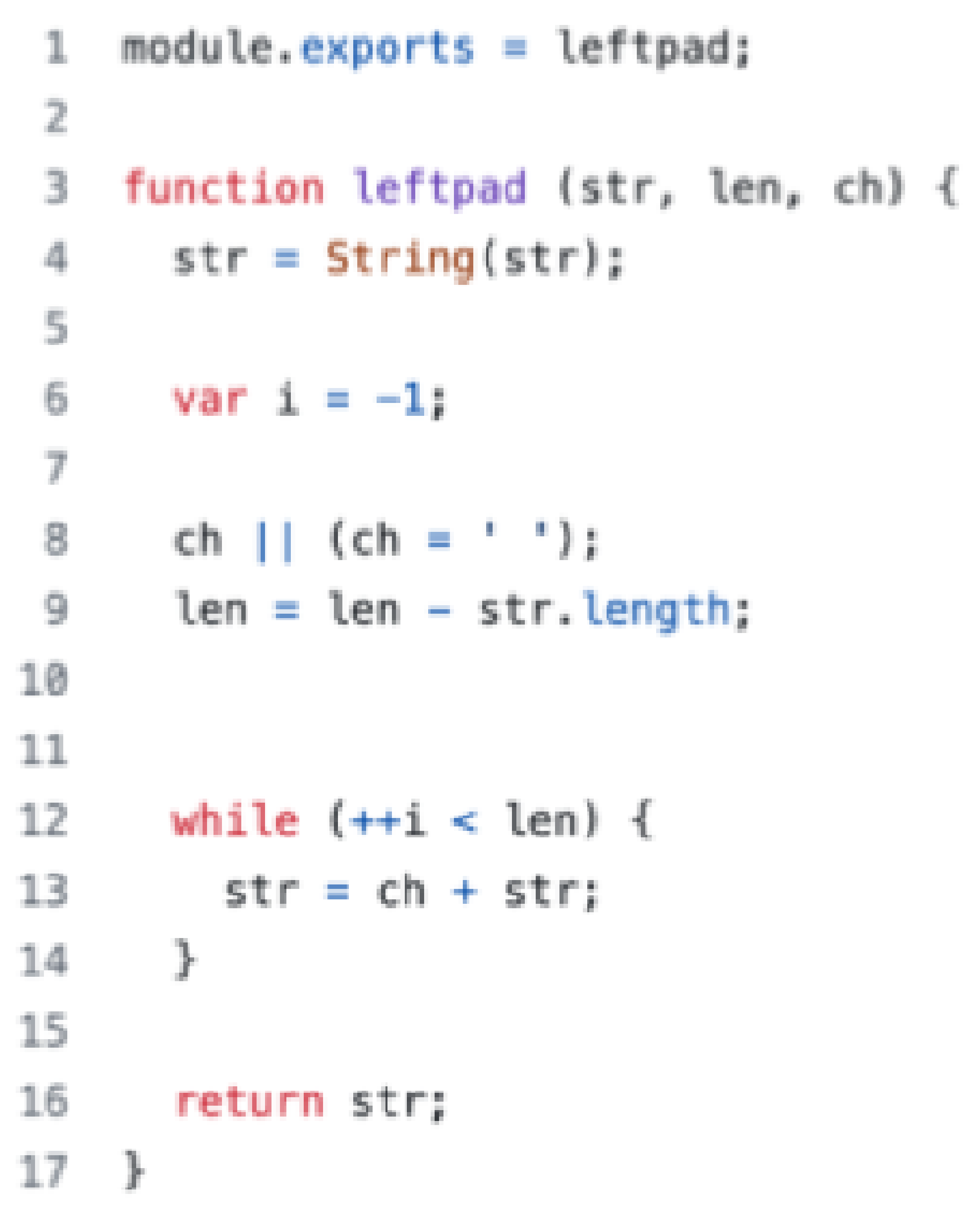
npm packages have a history, years ago it was leftpad, but because of frustration


LEFT-PAD
NPM
A STABLE PACKAGES ECOSYSTEM
imgflip.com

WHO WOULD WIN?

Multi-billion dollar corporations

11 lines of code



```
module.exports = leftpad;

function leftpad (str, len, ch) {
  str = String(str);

  var i = -1;

  ch || (ch = ' ');
  len = len - str.length;


  while (++i < len) {
    str = ch + str;
  }

  return str;
}
```

Back to xz

xz is a compression algorithm

and is included in ssh for some feature (I dont know)

A struggling developer

xz had a sole maintainer and when someone named Jia Tan helped him, he was relieved!

In fact, he had been scoffed online in recent months by people saying he was too slow in developing xz.

Finally some help to keep the online people happy

But it was Jia Tan all along

that made him feel this inadaquate

Then Jia Tan got to work with his master plan

He would insert a tricky mechanism that would compromise SSH

When SSH got build with this new version of XZ

The way he did it: Genius

The payload hidden with a unit test (!!!)

That test justify a weird binary, and that would be inserted in the executable at build time

All XZ code was alright, and who would read test code???

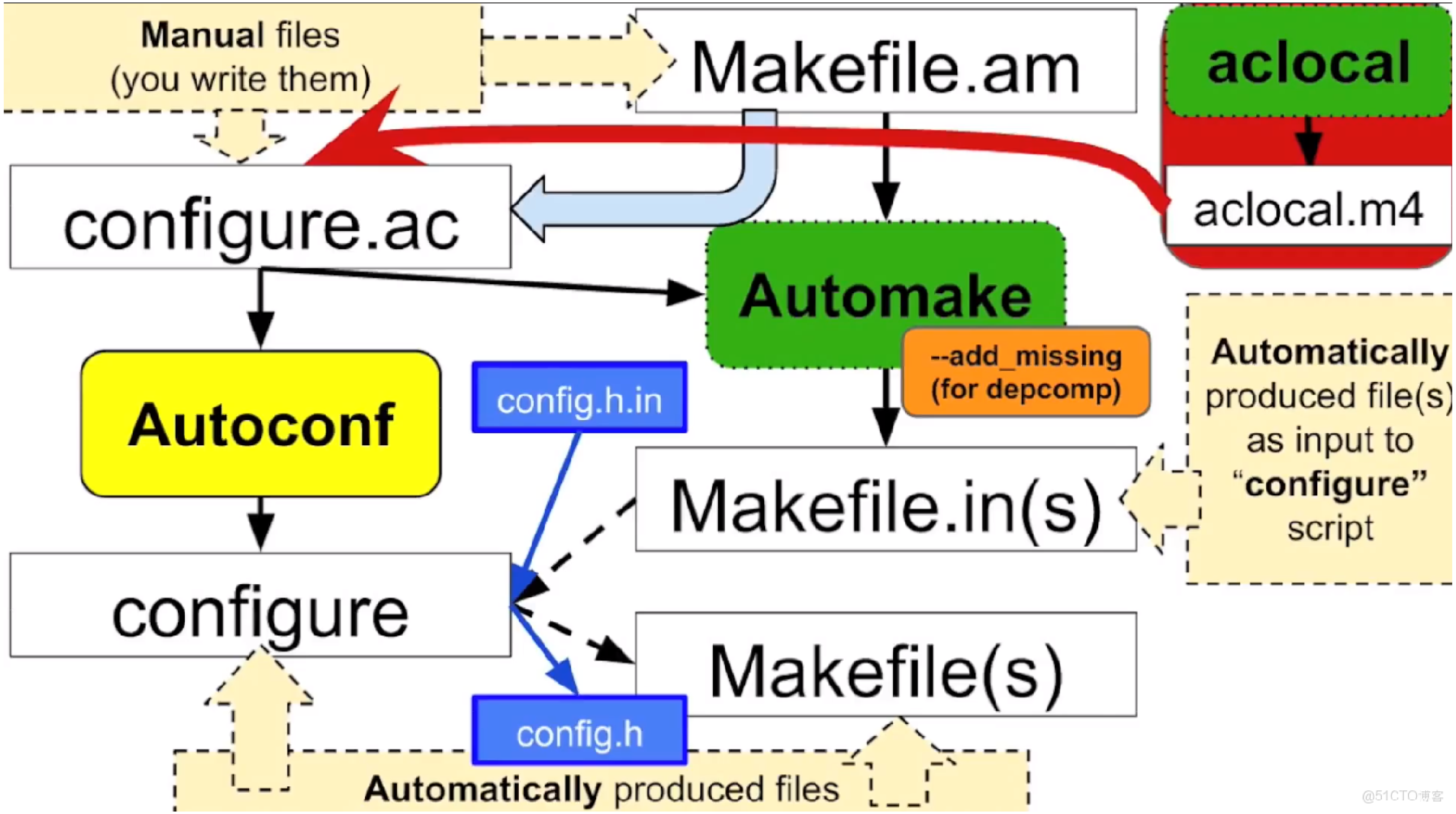
Obscure build tool chains

Also XZ is written in C and C has horrible build tool chains

Just as test code, how reads build tool chain code?

Now you say: dont use C, but so many stuff we use, all in C.

Андрей aka GNU Autotools
передает тебе привет
meme-arsenal.ru



Manual files
(you write them)

Makefile.am

aclocal

aclocal.m4

configure.ac

Automake

--add_missing
(for depcomp)

Autoconf

config.h.in

Makefile.in(s)

Automatically
produced file(s)
as input to
"**configure**"
script

configure

Makefile(s)

config.h

Automatically produced files

The backdoor itself: Equally Genius

SSH blocks login requests

But Jia Tan's backdoor sometimes like you would have the right credentials

Logs show: Blocked request

But secretly: Jia Tan is inside

And it only works if you have to key

This backdoor even uses the RSA encryption

Even if you know the backdoor exists, only Jia Tan has the keys

Discovered

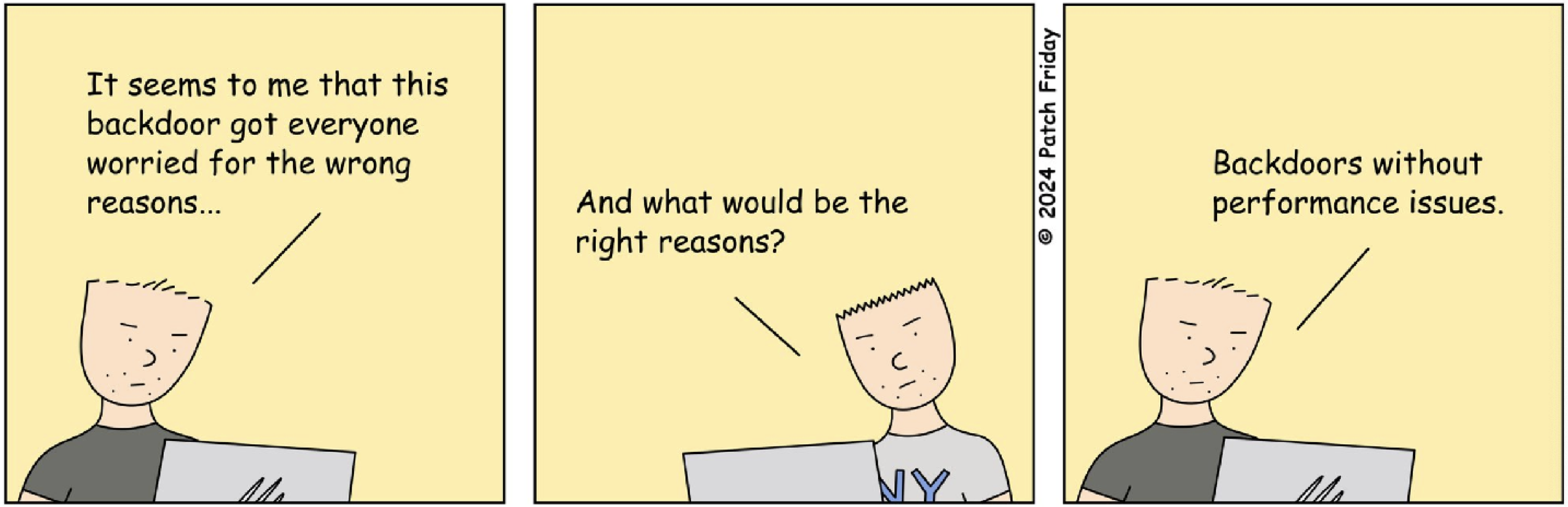
Someone tested the performance of SSH

Stripped a test environment to its essentials

Found a slowdown and investigated

However, the slowdown was in fact programming error on Jia Tan's side

XZ Utils Backdoor


It seems to me that this backdoor got everyone worried for the wrong reasons...
And what would be the right reasons?
NY
Backdoors without performance issues.

© 2024 Patch Friday

*Programmers
When a girl flirts
notice a library running 0.2s slower
made with mematic

The oppurtunity was closing

This genius making a mistake?

Jia Tan had all the possiblities to have this the most secret backdoor ever done

But, maybe he was in a hurry

SSH considering using a different dependency then XZ

Linux kernel developers preventing loading unneeded dependencies

Or maybe management (or a dictator) just wanted to get it done

So everything got fixed

But who is / or who are Jia Tan?

Or Jia Cheong Tan (CIA Agent John)

Working in UTC+2/UTC+3 (Russia/Ukraine/Israel)

Not working during Christmas

We do not know

How to protect yourself

There is a kill switch:

yolAbejyiejuvnup=Evjtgvsh5okmkAvj

Even though you would really need the key to open the backdoor