What’s the big deal with Confidential Computing?

Mike Bursell, CEO & Co-founder, Profian

STATE OF OPEN CON™23

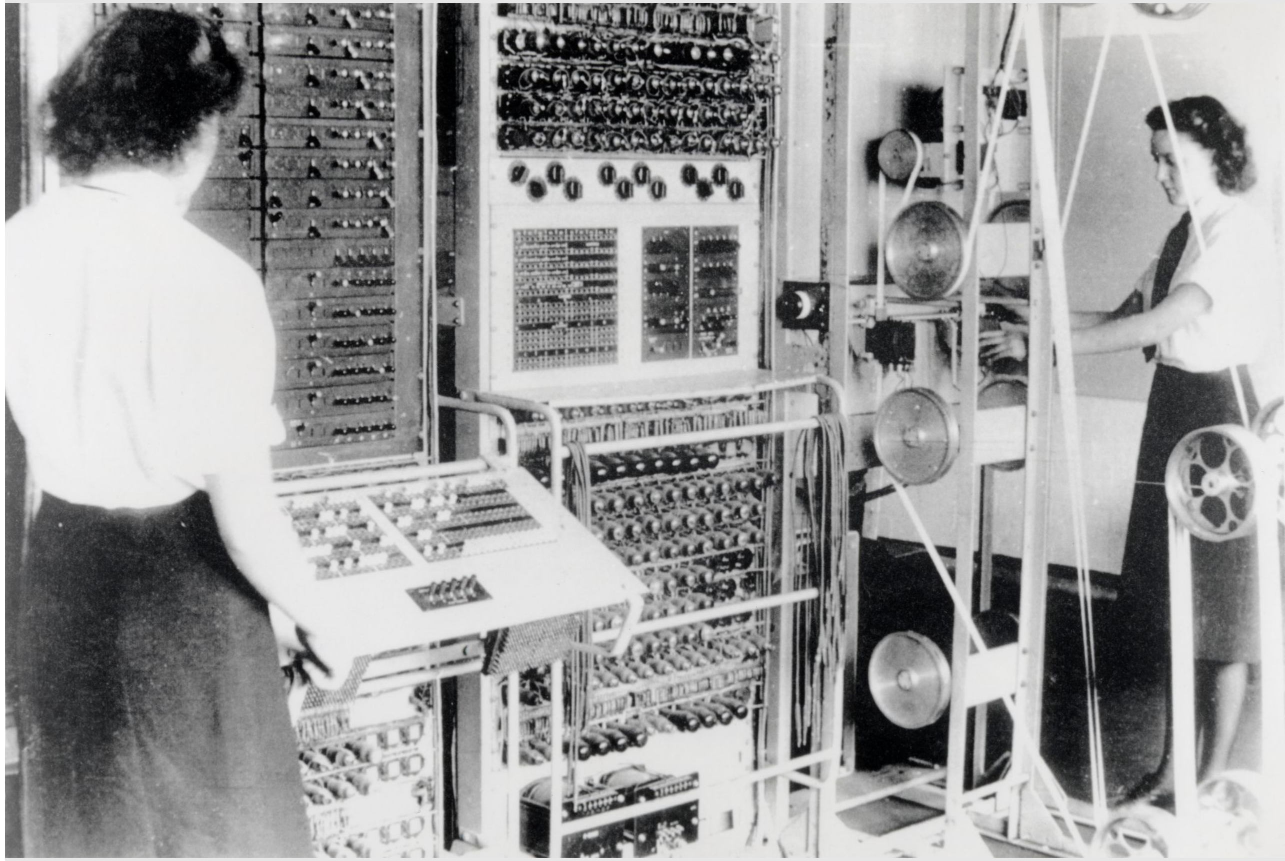
https://stateofopencon.com/ #stateofopencon #soocon23 #openuk
https://hachyderm.io/@openuk

The problem

Let me tell you a story...

Once upon a time,

Computing was simple. Computing was safe.



Once upon a time,

Computing was simple. Computing was safe.

And then along came the Brits.

Once upon a time,

Computing was simple. Computing was safe.

And then along came the Brits.

Who messed it all up.

Once upon a time,

Computing was simple. Computing was safe.

And then along came the Brits.

Who messed it all up.

Royally.

The importance of tea (and cake)

Image credit: MaltaGC - Photographed at the Great Central Railway, Loughborough.

The importance of tea (and cake)

Image credits: MaltaGC

It started with LEO III

LEO III/1 at Hartree House, April 1962
© Anthony Blake Photography
DCMLEO20190719002

Peter Bird Collection
LEO Computers Society Archive at the
Centre for Computing History, Cambridge
www.computinghistory.org.uk

It started with LEO III

The evil geniuses at LEO came up with a clever idea:

Multitasking

LEO III/1 at Hartree House, April 1962
© Anthony Blake Photography
DCMLEO20190719002

Peter Bird Collection
LEO Computers Society Archive at the
Centre for Computing History, Cambridge
www.computinghistory.org.uk

Ever since, people have been obsessed with sharing.

Ever since, people have been obsessed with sharing.

This is not a good thing

(for cake or computer security)

Image: By Maruf Hossain - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=106764918

The problem - computers

The problem - computers workloads

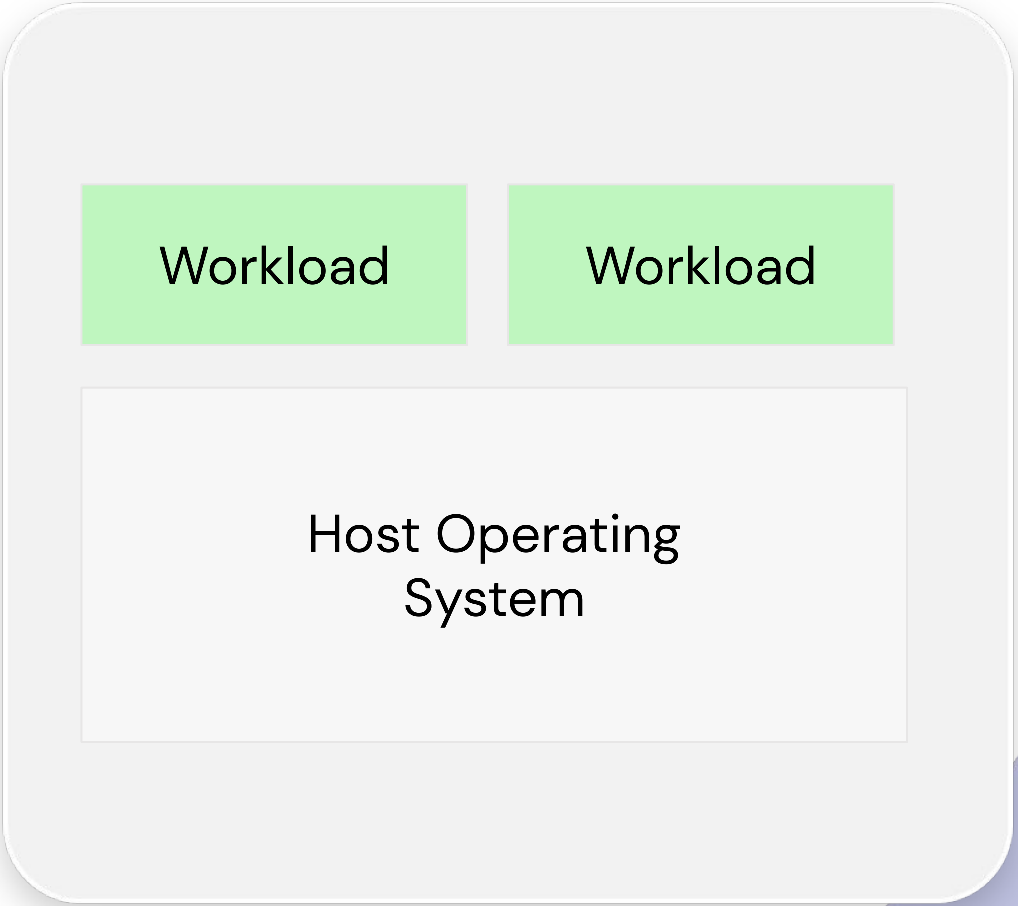
Standard virtualization model

Isolation is important - but what is it?

One model: CIA triad

- Confidentiality
- Integrity
- Availability

Generally, *availability* is easily observed



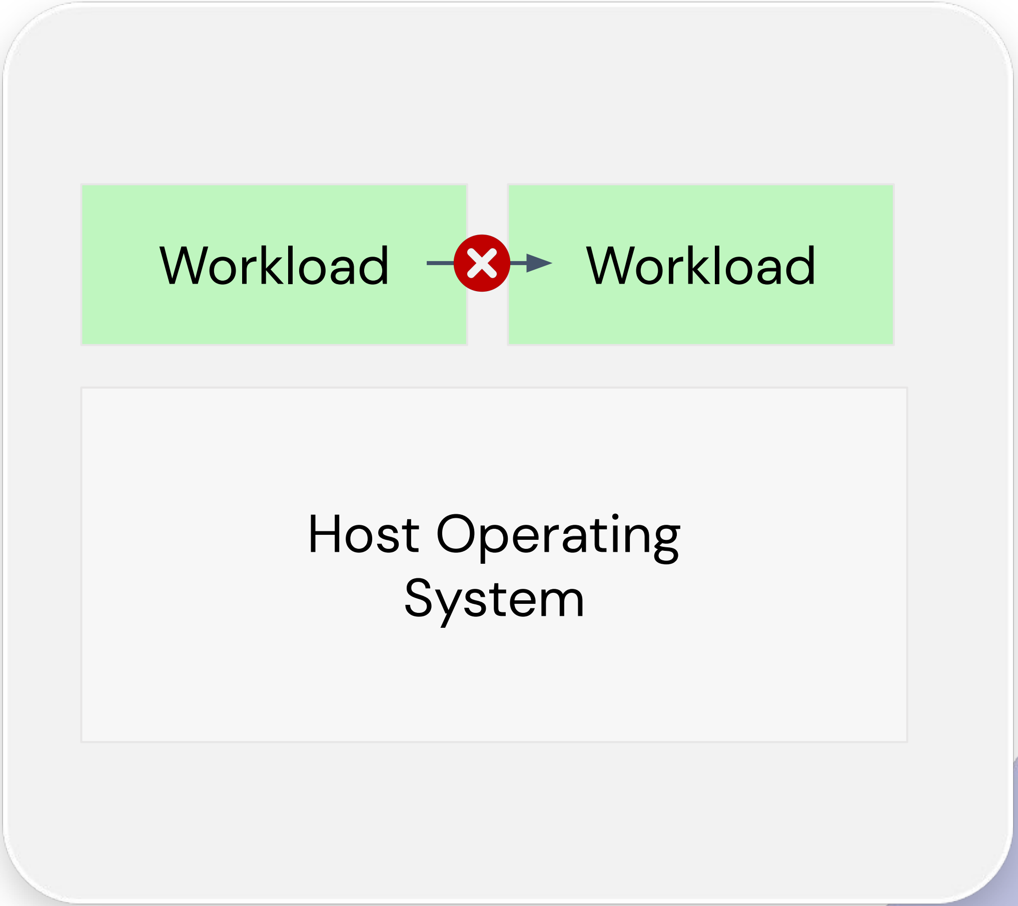
The problem - computers workloads

Standard virtualization model

TYPE 1

Workload from workload isolation

VMs and containers handle this pretty well



The problem - ~~computers~~ workloads

Standard virtualization model

TYPE 1

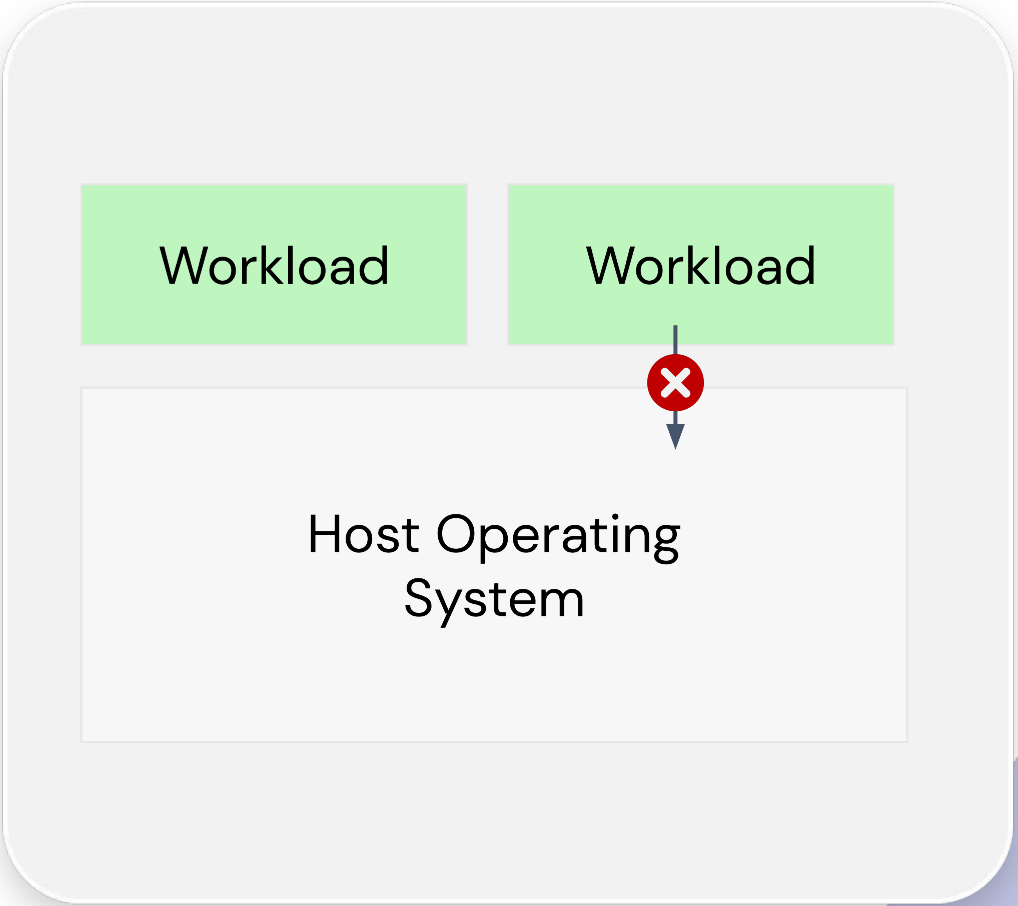
Workload from workload isolation

VMs and containers handle this pretty well

TYPE 2

Host from workload isolation

VMs and containers handle this pretty well



The problem - computers workloads

Standard virtualization model

TYPE 1

Workload from workload isolation

VMs and containers handle this pretty well

TYPE 2

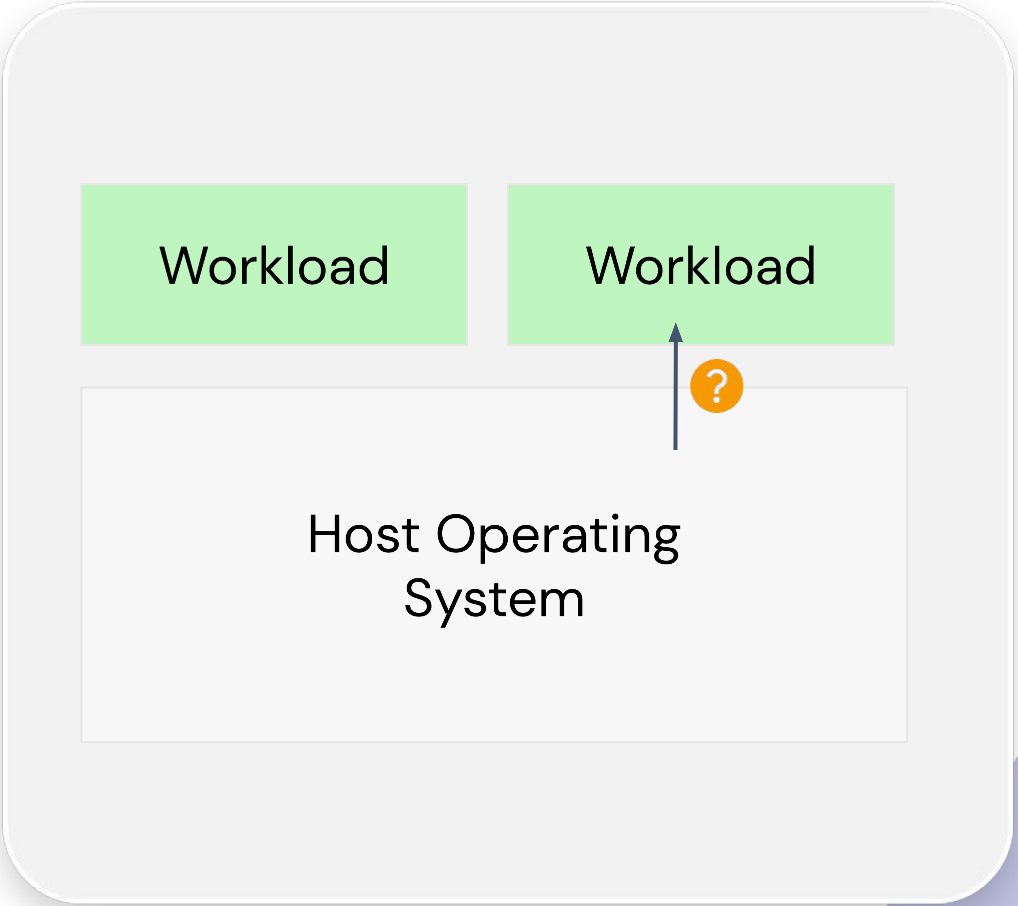
Host from workload isolation

VMs and containers handle this pretty well

TYPE 3

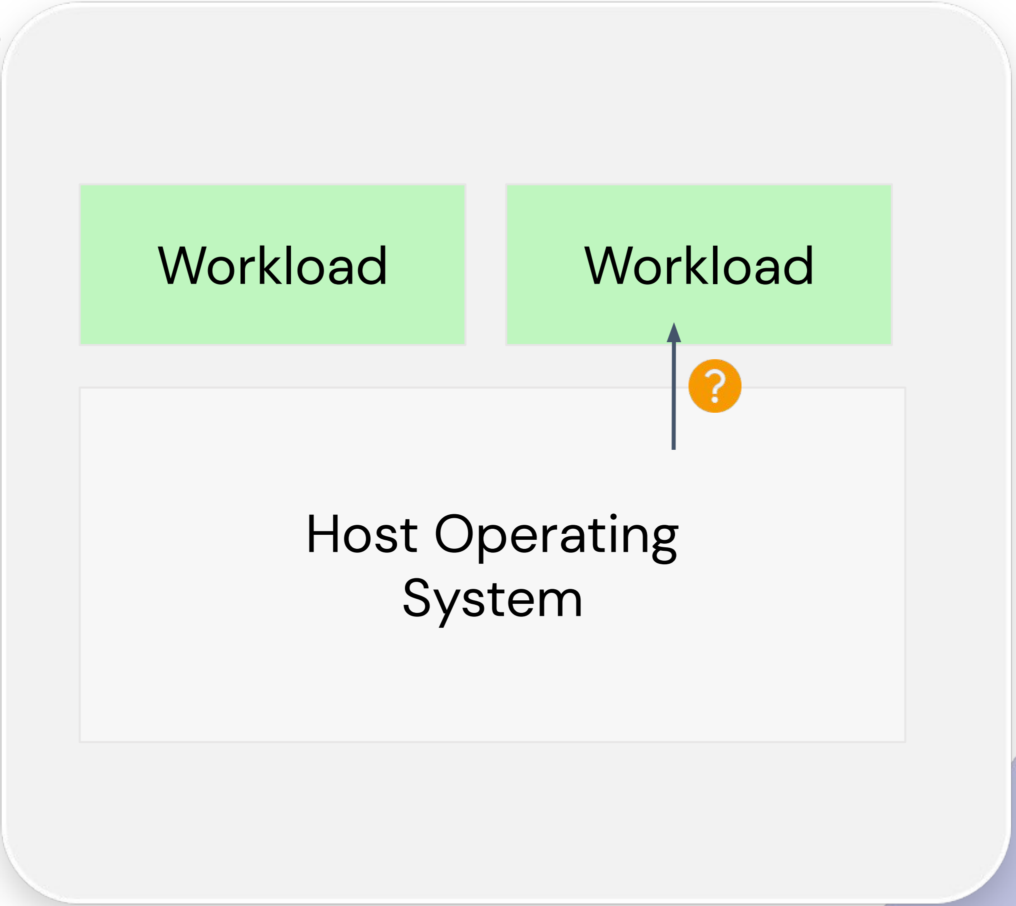
Workload from host isolation

Classical virtualization **cannot** provide this



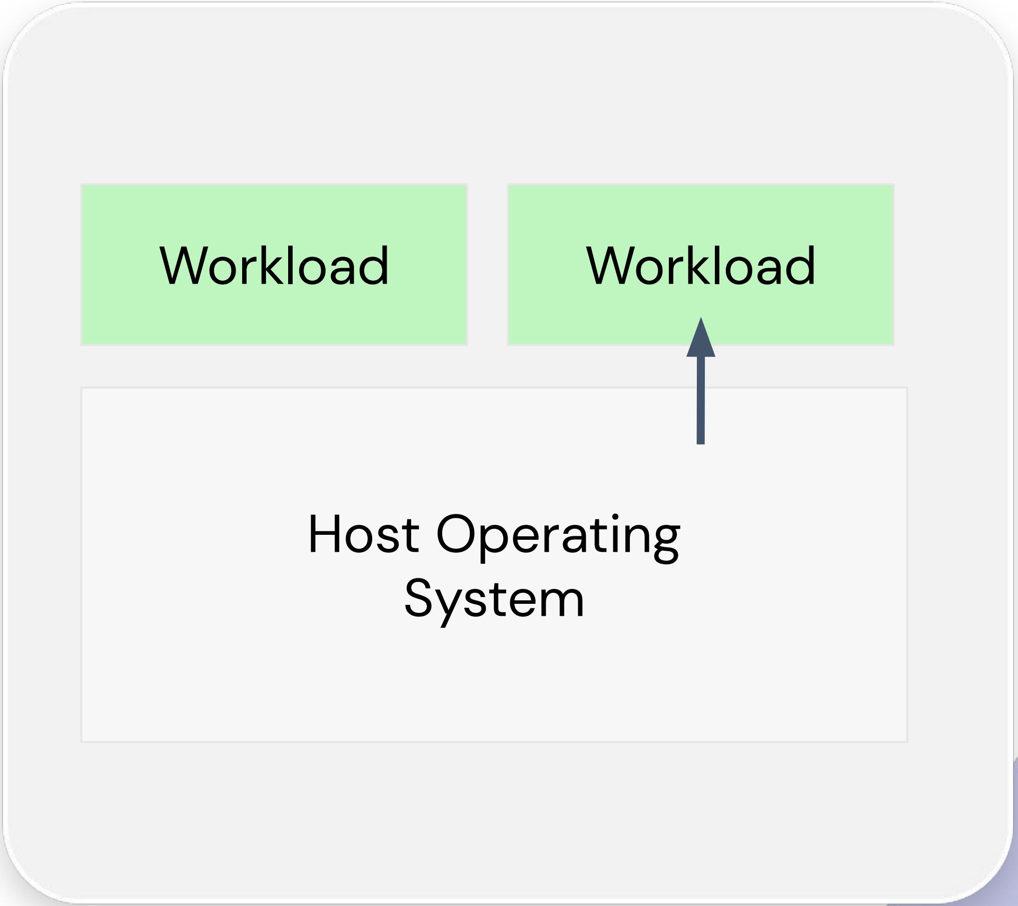
Cloud and Edge

What about the Cloud (and the Edge)?



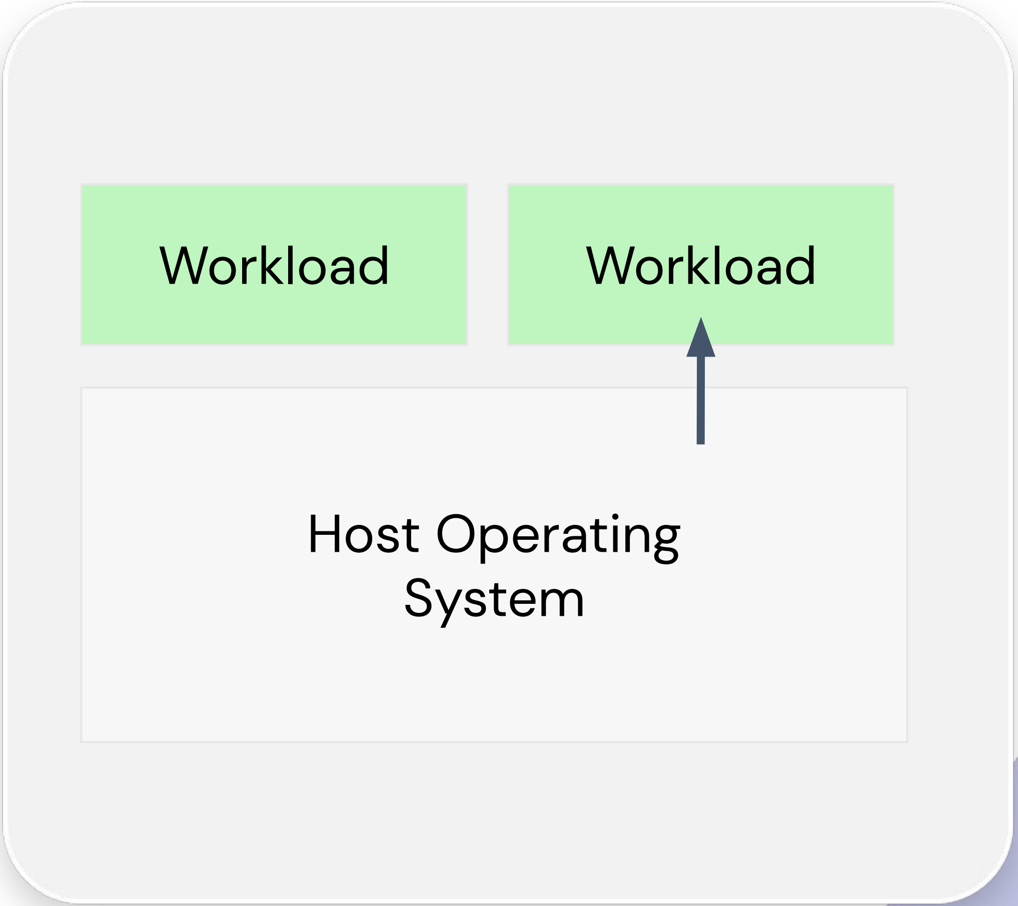
Cloud and Edge

- Well, this is awkward



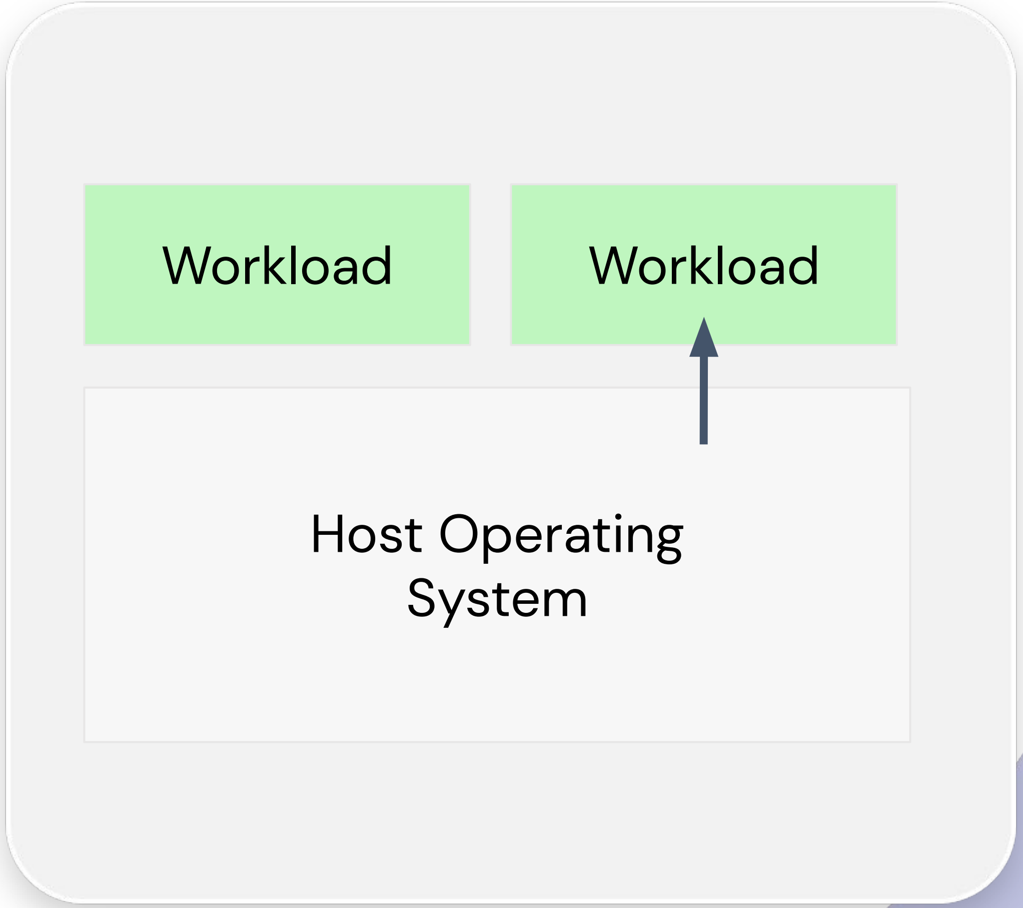
Cloud and Edge

- Well, this is awkward
- Of course it's OK…



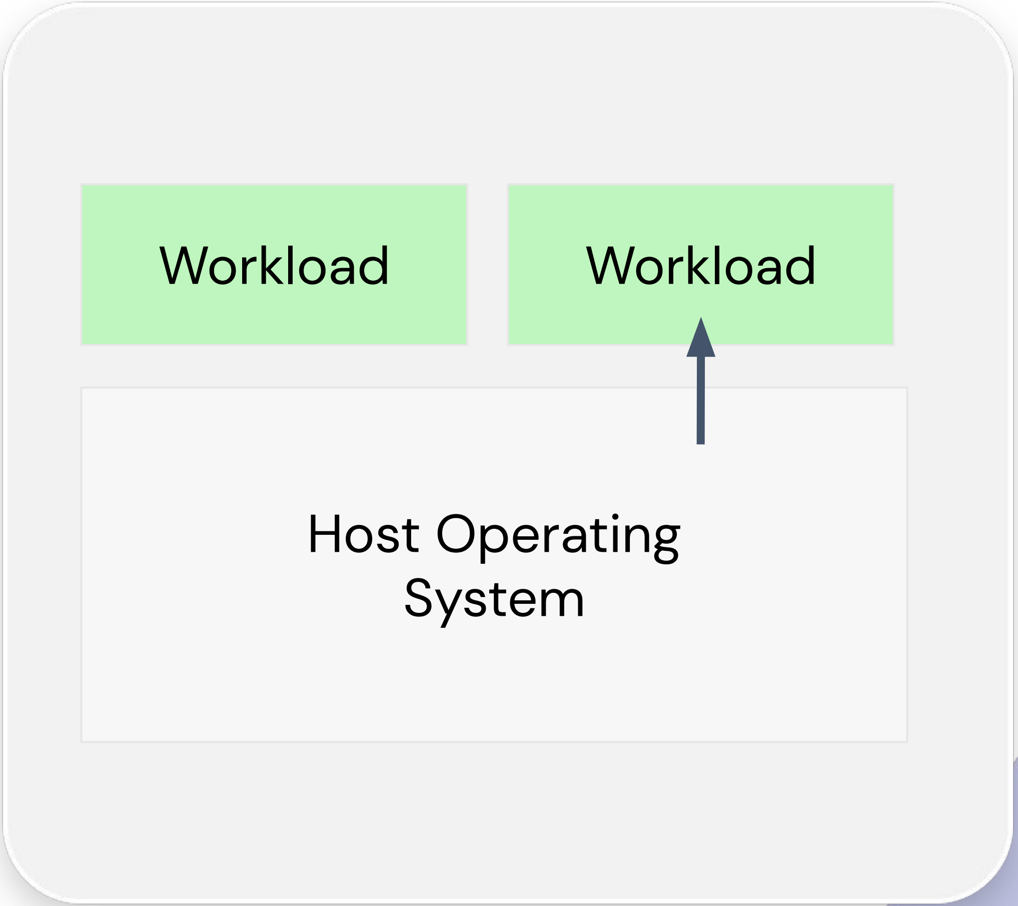
Cloud and Edge

- Well, this is awkward
- Of course it's OK…
  - If you trust your CSP



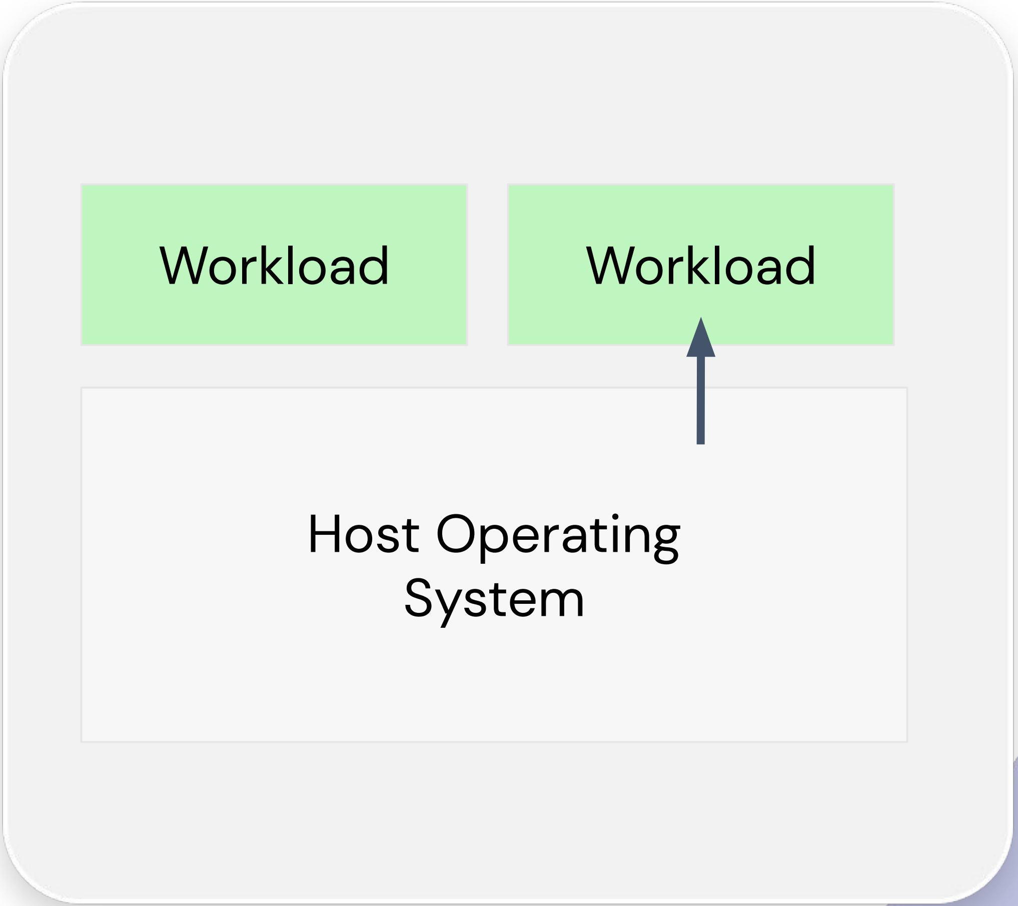
Cloud and Edge

- Well, this is awkward
- Of course it’s OK…
  - If you trust your CSP
  - And all of their sysadmins



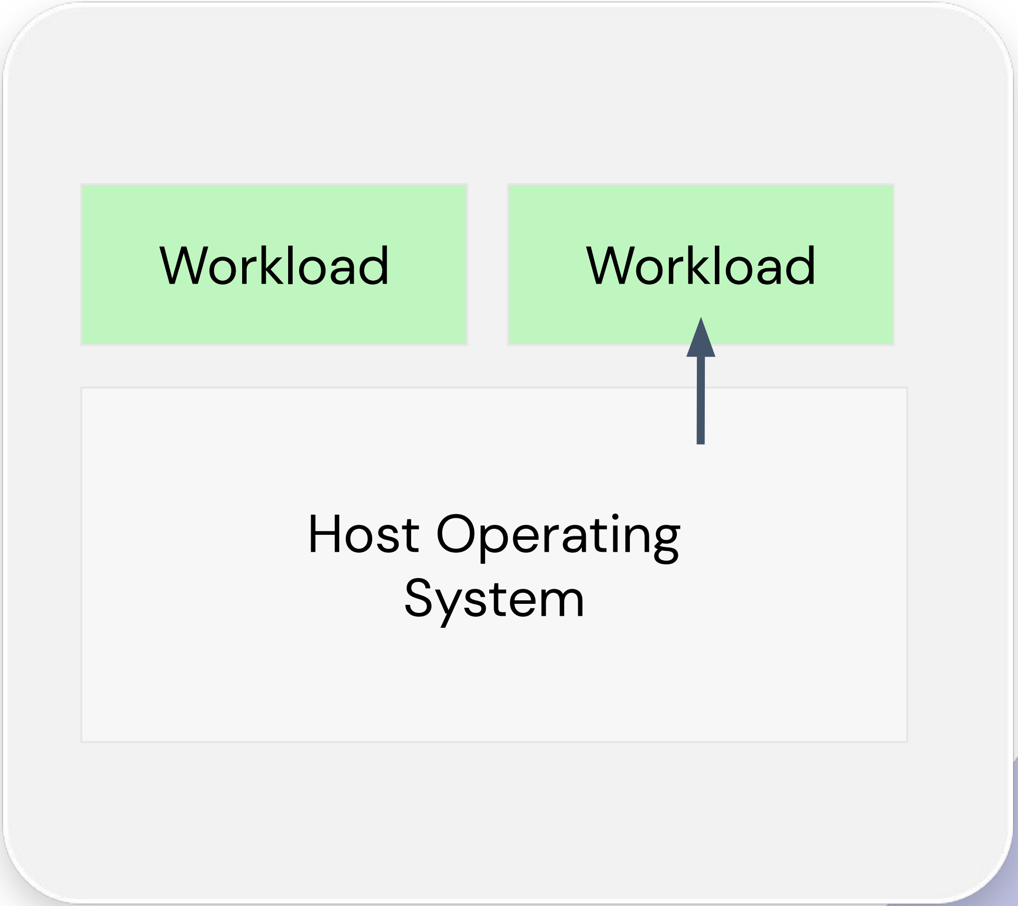
Cloud and Edge

- Well, this is awkward
- Of course it’s OK…
  - If you trust your CSP
  - And all of their sysadmins
  - And all of the hardware, software & firmware stack
  - From compromise



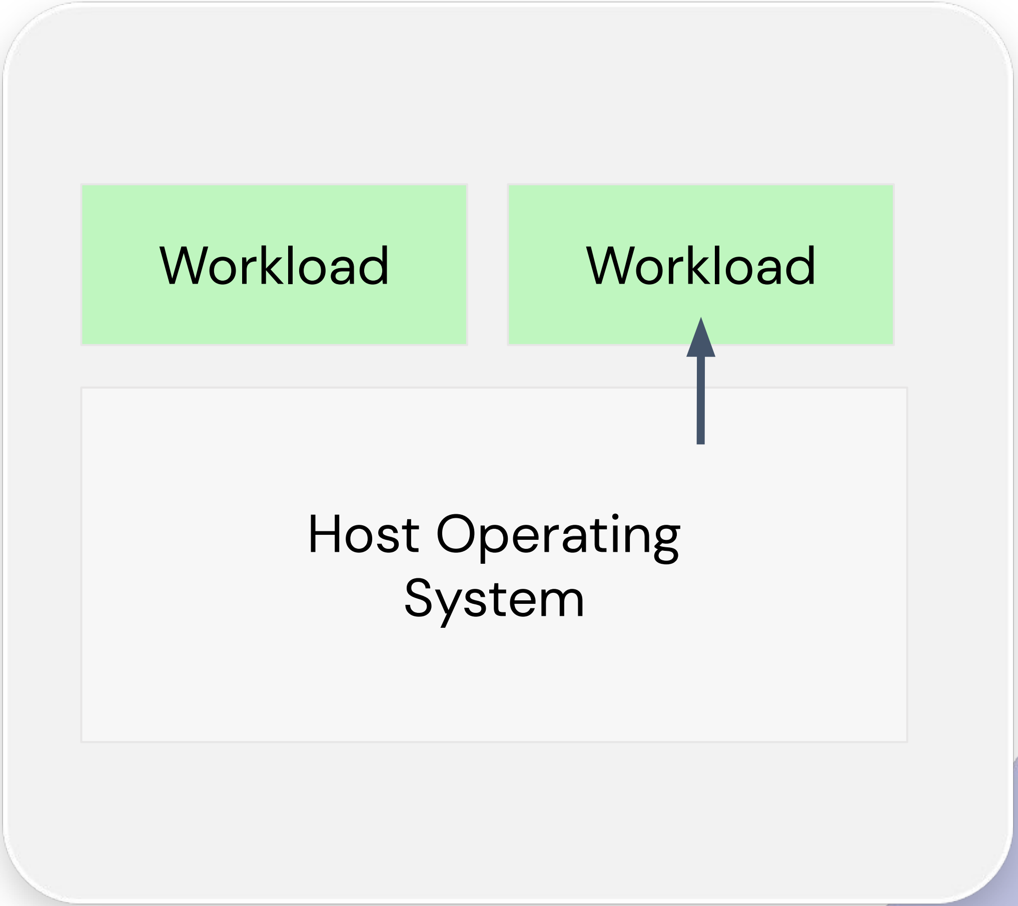
Cloud and Edge

- Well, this is awkward
- Of course it's OK…
  - If you trust your CSP
  - And all of their sysadmins
  - And all of the hardware, software & firmware stack
  - From compromise
  - Of supply chain or at runtime



Cloud and Edge

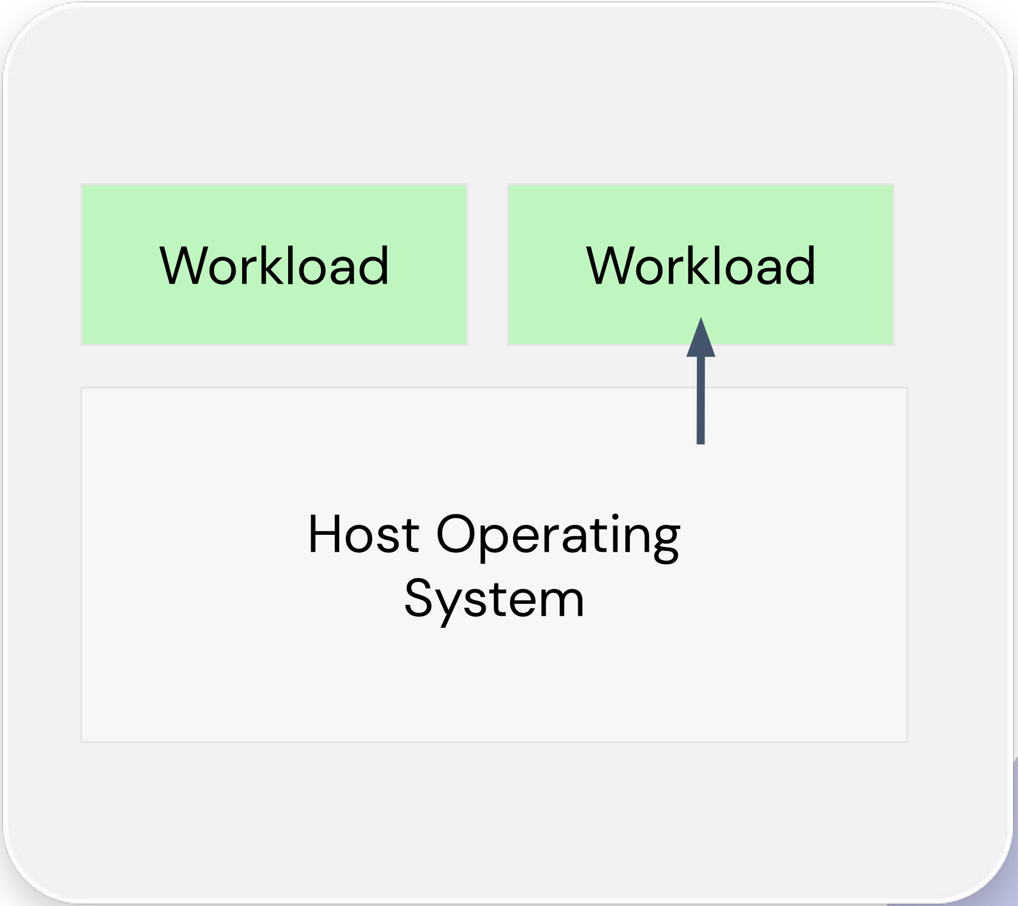
- Well, this is awkward
- Of course it's OK…
  - If you trust your CSP
  - And all of their sysadmins
  - And all of the hardware, software & firmware stack
  - From compromise
  - Of supply chain or at runtime
  - Now and in the future



Cloud and Edge

- Well, this is awkward
- Of course it's OK…
  - If you trust your CSP
  - And all of their sysadmins
  - And all of the hardware, software & firmware stack
  - From compromise
  - Of supply chain or at runtime
  - Now and in the future

And your CFO and board and auditor and regulator all do, as well



STATE OF OPEN CON™ 23

Cloud and Edge

- Well, this is awkward
- Of course it’s OK…
  - If you trust your CSP
  - And all of their sysadmins
  - And all of the hardware, software & firmware stack
  - From compromise
  - Of supply chain or at runtime
  - Now and in the future

And your CFO and board and auditor and regulator all do, as well

Cloud and Edge

- Well, this is awkward
- Of course it's OK…
  - If you trust your CSP
  - And all of their sysadmins
  - And all of the hardware, software & firmware stack
  - From compromise
  - Of supply chain or at runtime
  - Now and in the future

And your CFO and board and auditor and regulator all do, as well

Not all clouds are good (sorry)

Confidential Computing introduction

Confidential Computing

“Confidential Computing is the protection of data in use by performing computation in an attested, hardware-based Trusted Execution Environment.”

- Confidential Computing Consortium

https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/03/CCC-Tech-Analysis-Confidential-Computing-V1.pdf

Confidential Computing

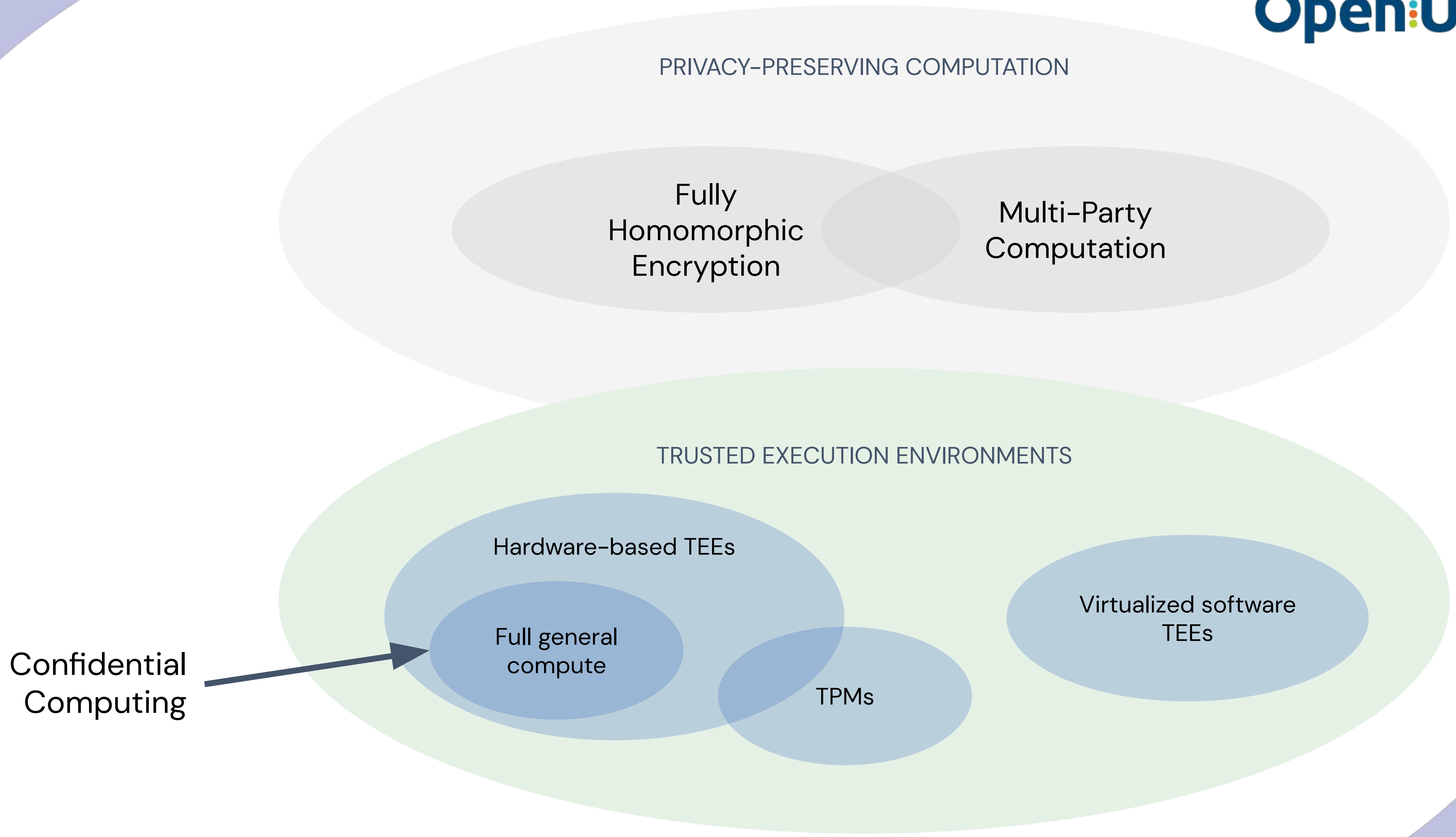
"Confidential Computing is the protection of data in use by performing computation in an attested, hardware-based Trusted Execution Environment."

- Confidential Computing Consortium

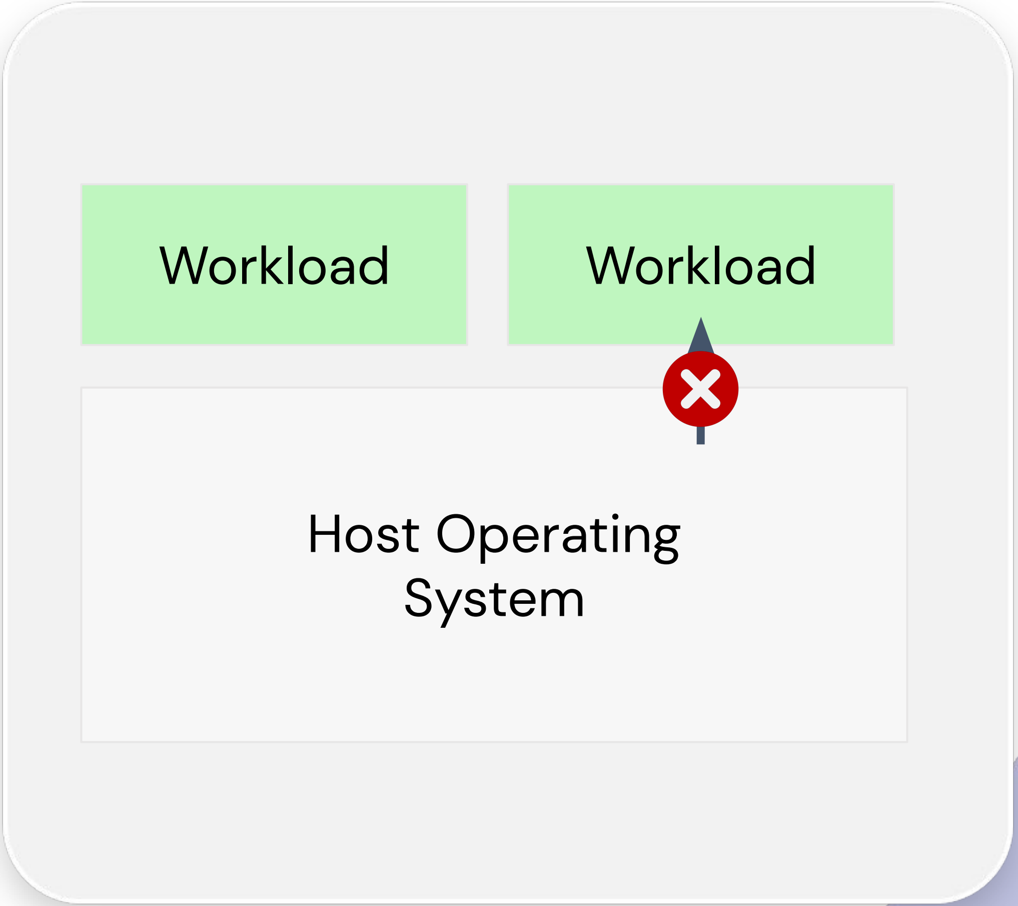
- Linux Foundation project
- Focused on open source software
- Broad industry adoption
  - Intel, AMD, Arm, Red Hat, Microsoft, Facebook, Accenture, Ant, Huawei, Google, Cisco, nVidia, VMware, Profian, ...

CONFIDENTIAL COMPUTING CONSORTIUM

https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/03/CCC-Tech-Analysis-Confidential-Computing-V1.pdf

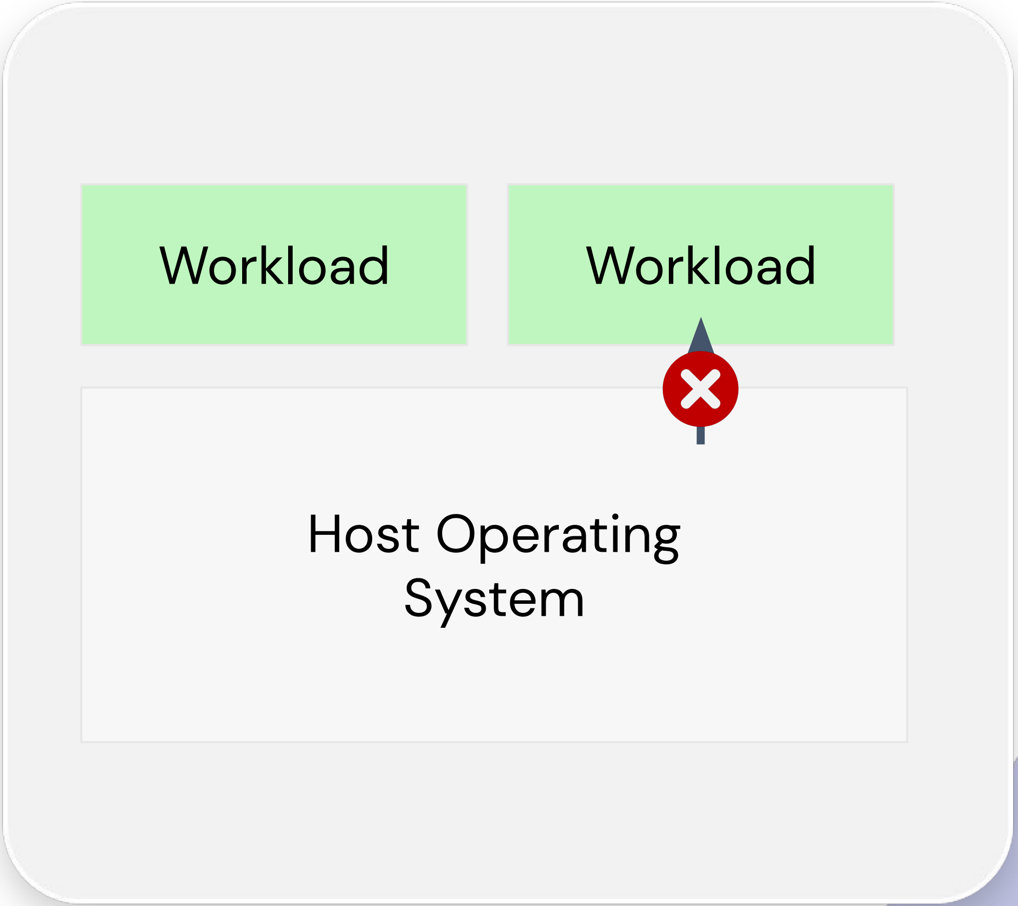

PRIVACY-PRESERVING COMPUTATION
Fully Homomorphic Encryption
Multi-Party Computation
TRUSTED EXECUTION ENVIRONMENTS
Hardware-based TEEs
Full general compute
TPMs
Virtualized software TEEs
Confidential Computing

Confidential Computing



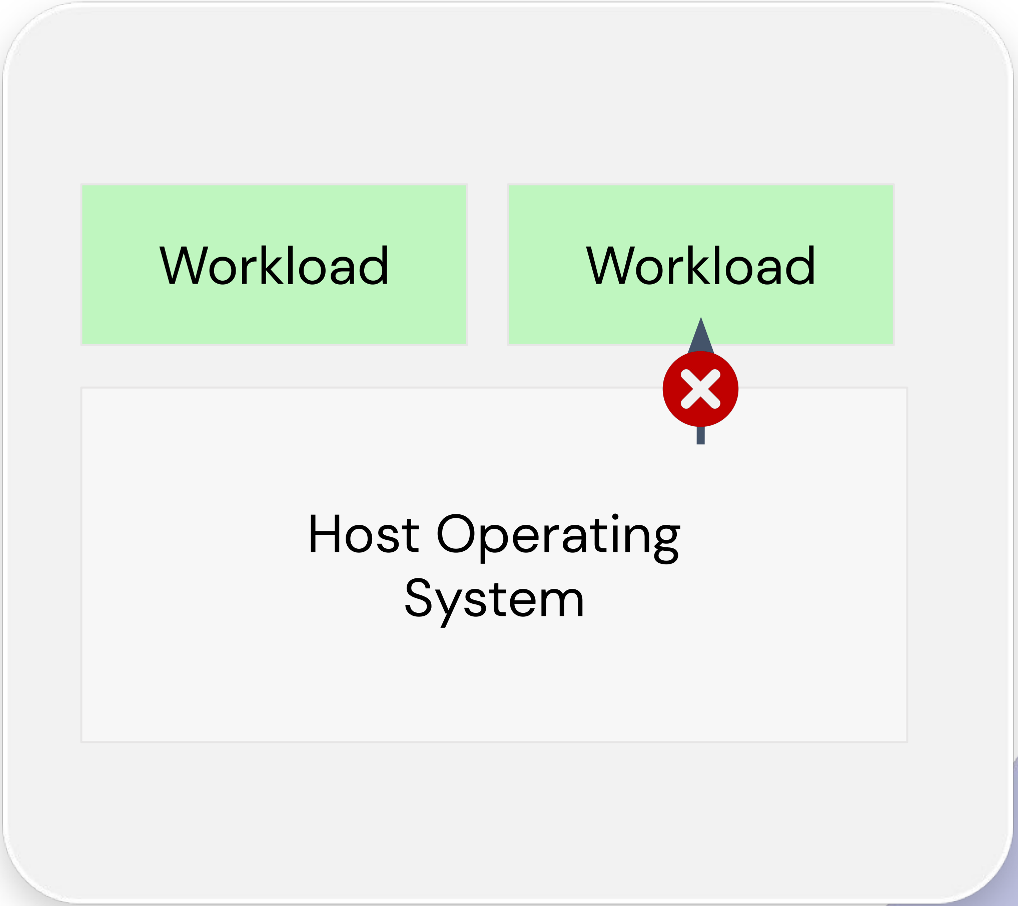
Confidential Computing

- Uses TEEs
  - Trusted Execution Environments
  - Based on CPUs (e.g. Intel SGX, AMD SEV)



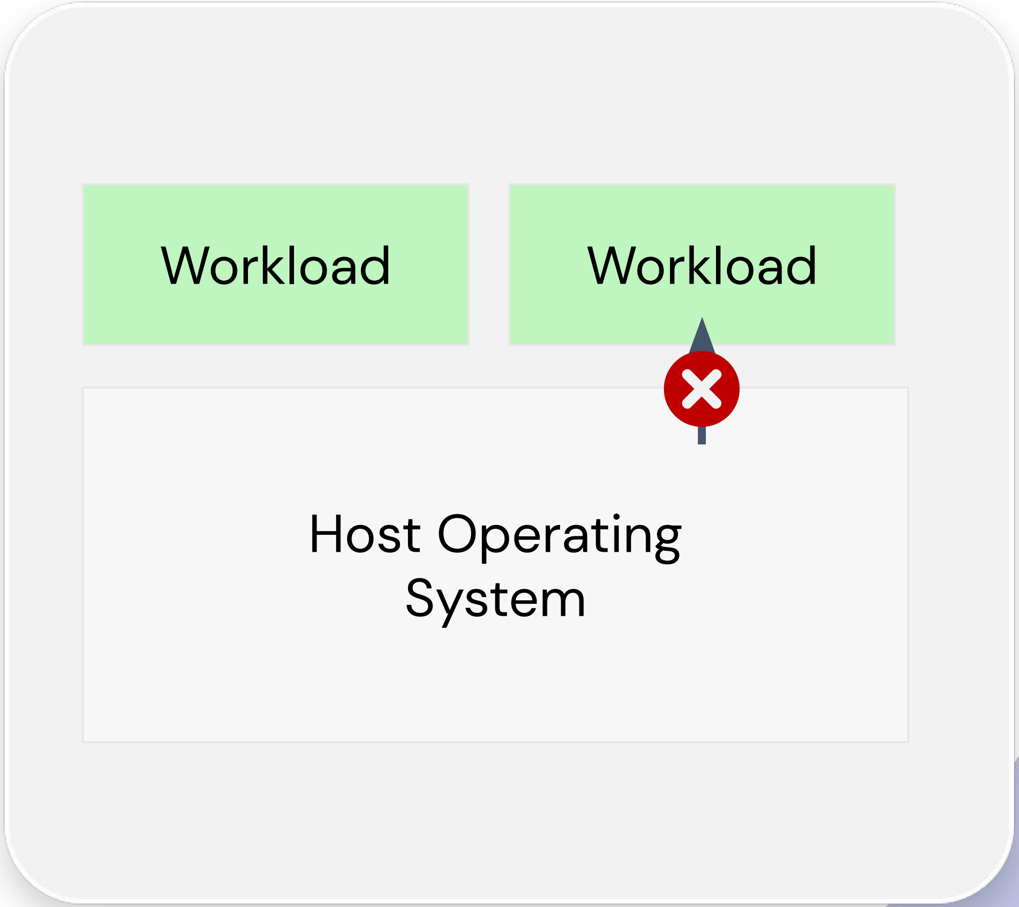
Confidential Computing

- Uses TEEs
  - Trusted Execution Environments
  - Based on CPUs (e.g. Intel SGX, AMD SEV)
- TEEs encrypt workloads



Confidential Computing

- Uses TEEs
  - Trusted Execution Environments
  - Based on CPUs (e.g. Intel SGX, AMD SEV)
- TEEs encrypt workloads
- TEEs protect
  - Integrity
  - Confidentiality



Confidential Computing is about deploying applications to TEEs.

Confidential Computing is about deploying applications to TEEs.

(Which is harder than you might think)

But first … is it really tea?

I love tea and cake

1. I’ve got some cake
2. I want to eat it with some tea
3. I call your cafe to order a pot of tea
4. You provide the pot
5. I’ll come with cake
6. BUT I can’t check the tea first

I love tea and cake

1. I’ve got some cake
2. I want to eat it with some tea
3. I call your cafe to order a pot of tea
4. You provide the pot
5. I’ll come with cake
6. BUT I can’t check the tea first

So, what if you provide a pot of coffee?

I love tea and cake

1. I've got some cake
2. I want to eat it with some tea
3. I call your cafe to order a pot of tea
4. You provide the pot
5. I'll come with cake
6. BUT I can't check the tea first

So, what if you provide a pot of coffee?

No!!!!

Image by Christoph from Pixabay

I love tea and cake

I need a remote, trusted tea taster

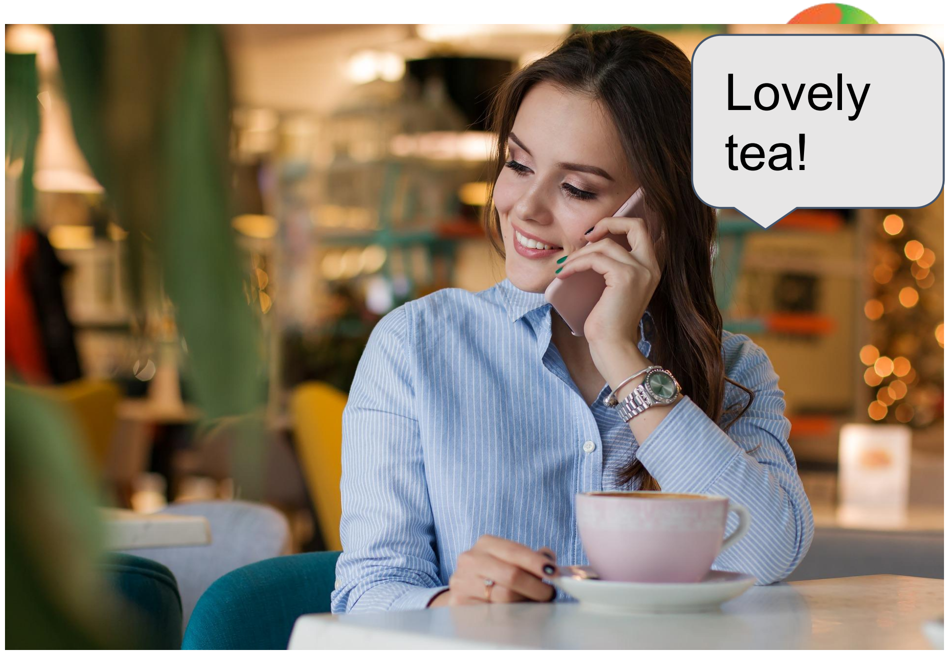
- Who can warn me ...
- … before I turn up with cake

Images by Anastasia Gepp from Pixabay

I love tea and cake

I need a remote, trusted tea taster

- Who can warn me ...
- … before I turn up with cake



Images by Anastasia Gepp from Pixabay

I love tea and cake

I need a remote, trusted tea taster

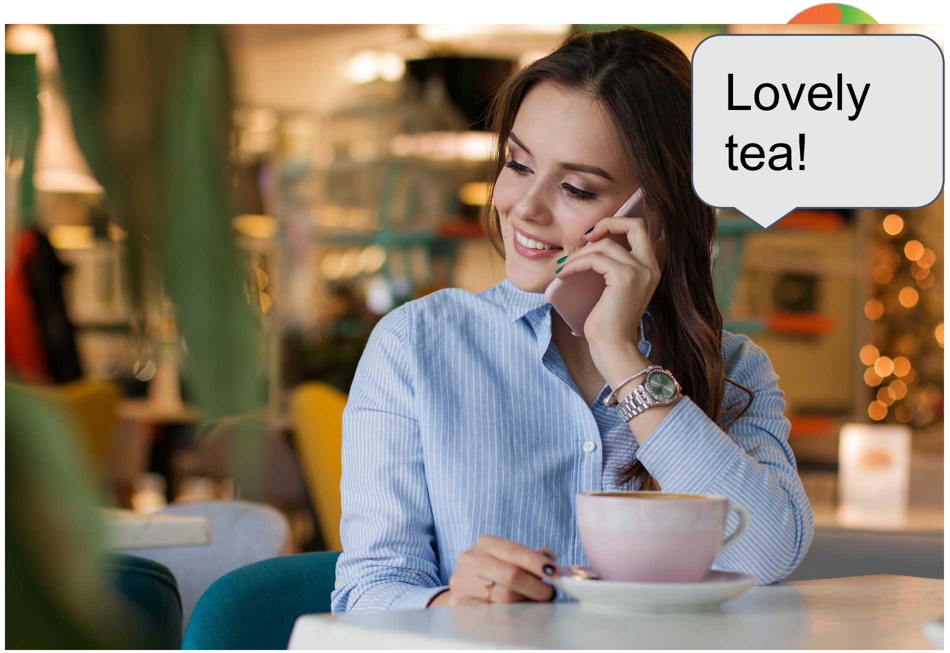
- Who can warn me ...
- … before I turn up with cake

Cafe = CSP’s machine

Tea = Trusted Execution Environment (TEE)

Coffee = Spoofed (fake) TEE

Cake = my workload and data



I love tea and cake

I need a remote, trusted tea taster

- Who can warn me
- Before I turn up with cake

Cafe = CSP’s host machine

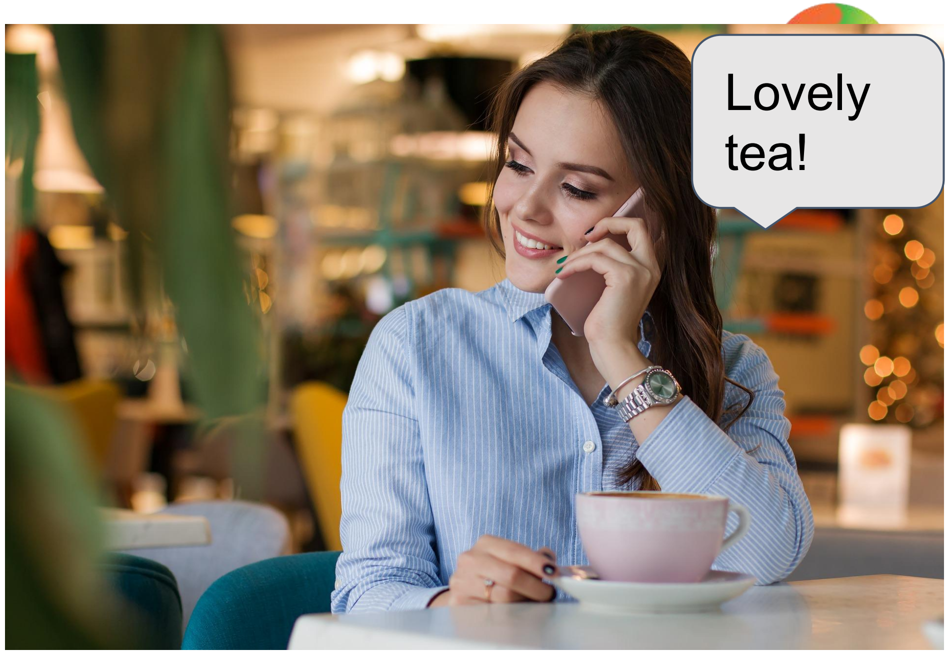
Sorry

Tea = Trusted Execution Environment

(TEE)

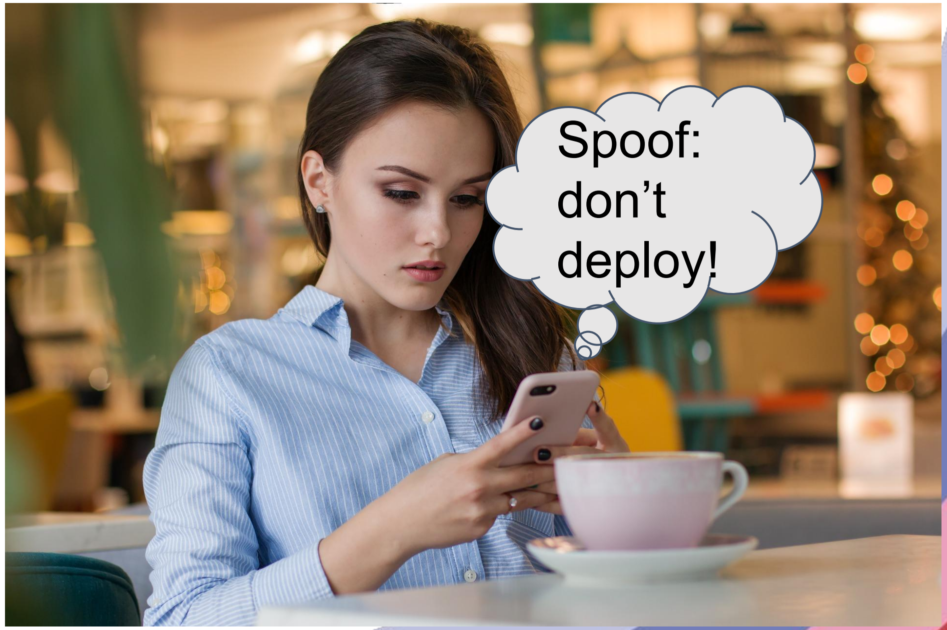
Coffee = Spoofed (fake) TEE

Cake = my workload and data



Attestation

The measurement of the TEE instance by a trusted entity and subsequent verification.

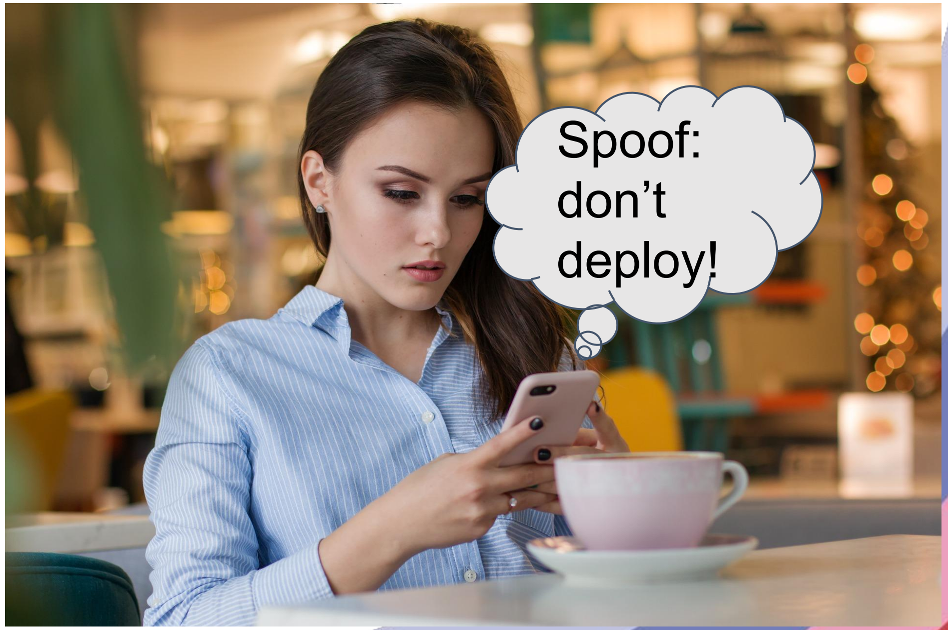


Attestation

The measurement of the TEE instance by a trusted entity and subsequent verification.

How do you find a trusted entity in the CSP?

- All hardware under CSP’s control
- All software under CSP’s control



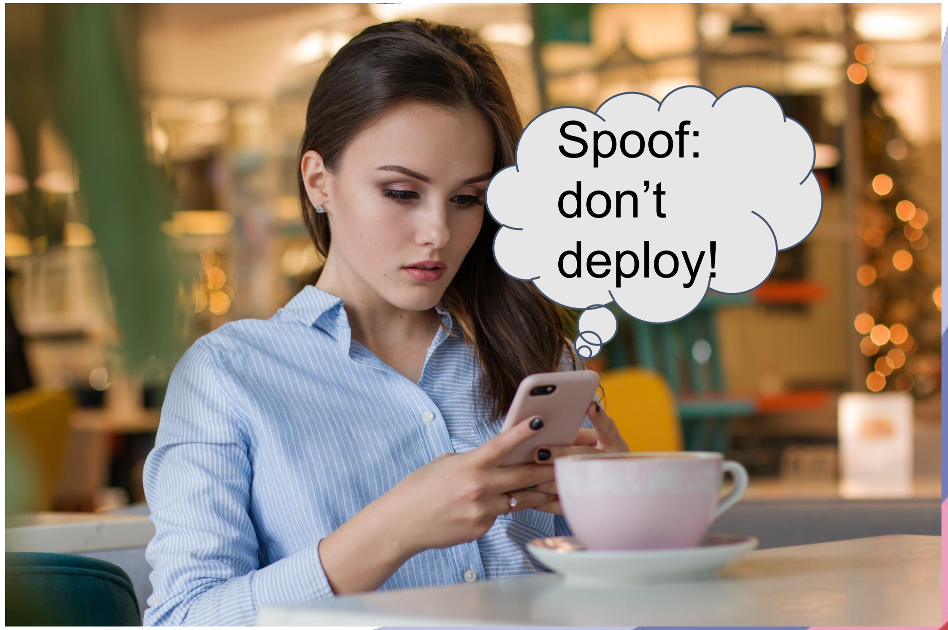
Attestation

The measurement of the TEE instance by a trusted entity and subsequent verification.

How do you find a trusted entity in the CSP?

- All hardware under CSP's control
- All software under CSP's control

Good news: CPU + firmware can measure and sign TEE + contents (memory pages)



Attestation

Actually

- Measurement is on CSP’s host (in cafe)

Image by Anastasia Gepp and congerdesign from Pixabay

Attestation

Actually

- Measurement is on CSP’s host (in cafe)
- Validation **must** be managed by a trusted entity

Image by Anastasia Gepp and congerdesign from Pixabay

Attestation

Actually

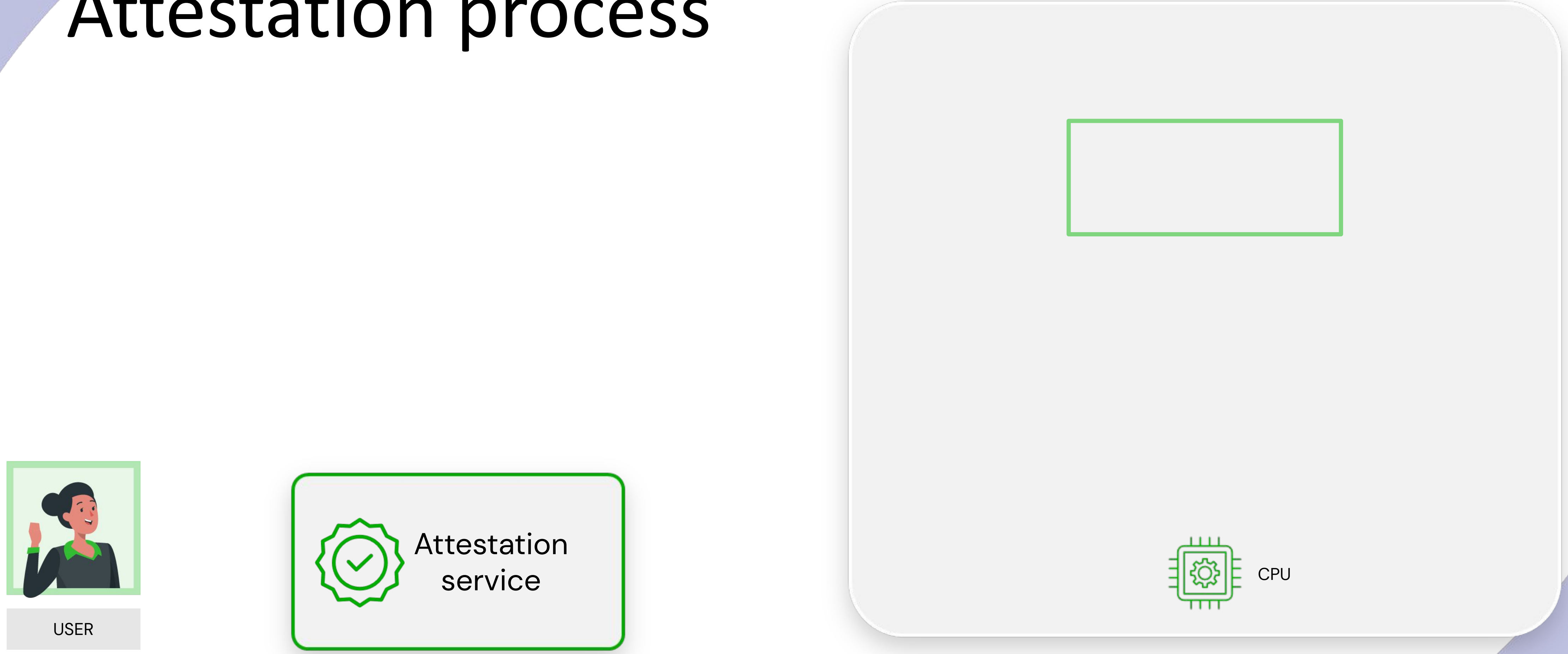
- Measurement is on CSP’s host (in cafe)
- Validation **must** be managed by a trusted entity
- You can then choose to deploy (or not)

This is very difficult to get right, and devastating if you do it wrong.

Image by Anastasia Gepp and congerdesign from Pixabay

Enough with the tea and cake metaphor!

Attestation process

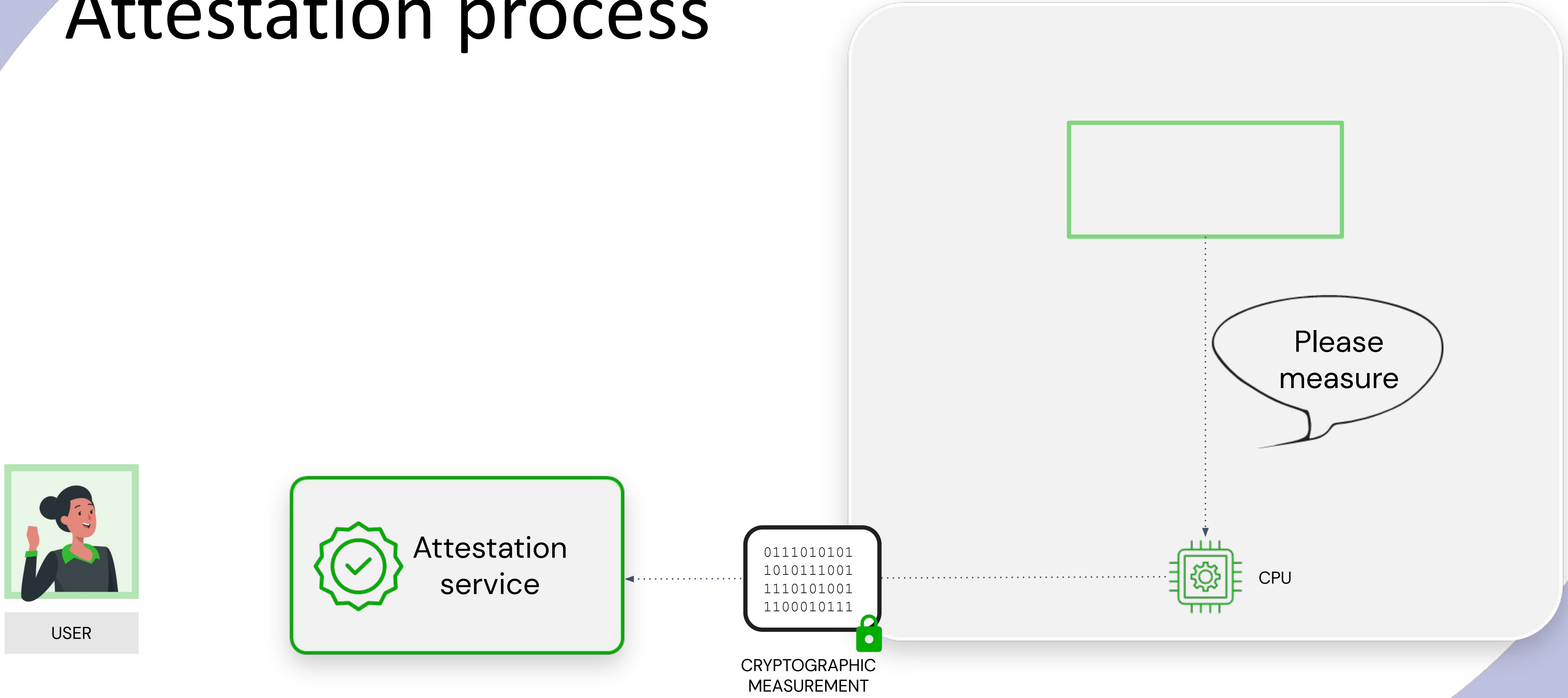


USER

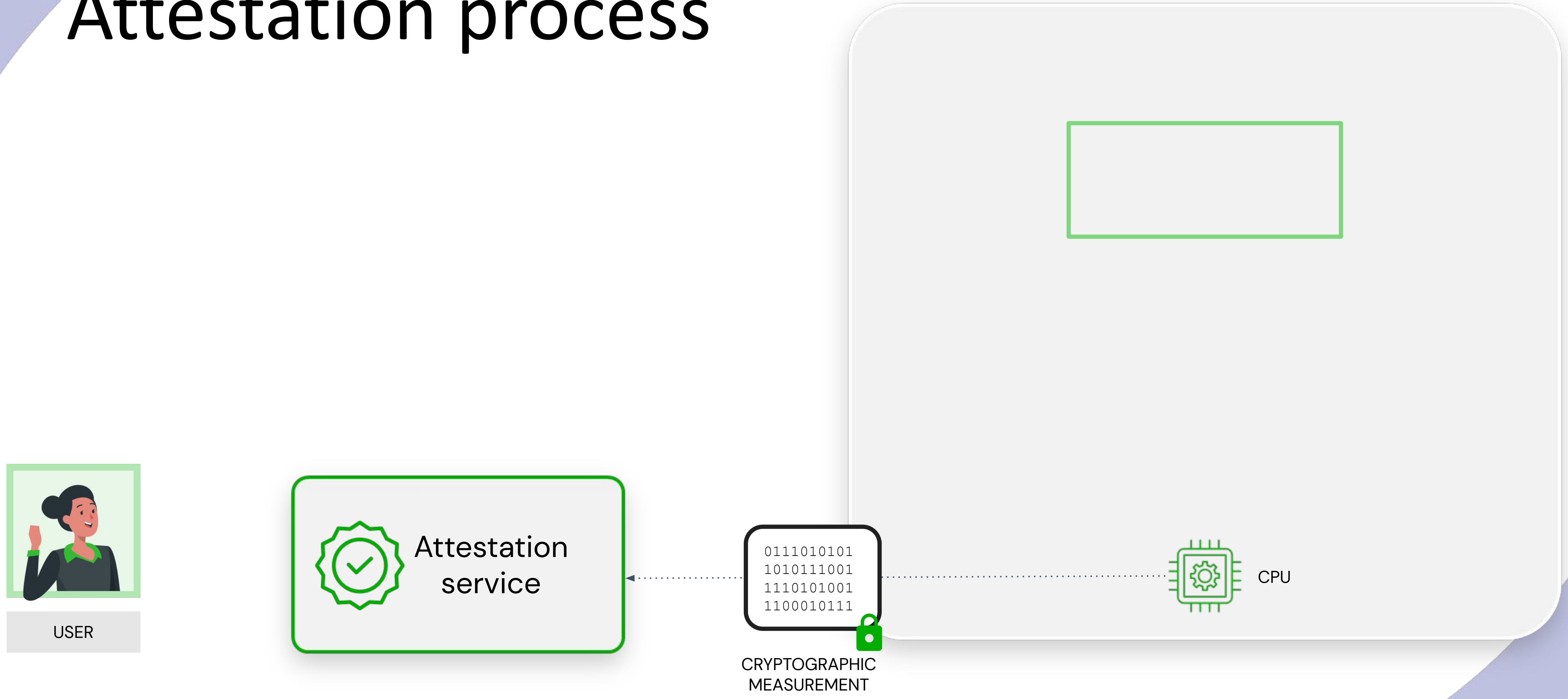
Attestation service

CPU

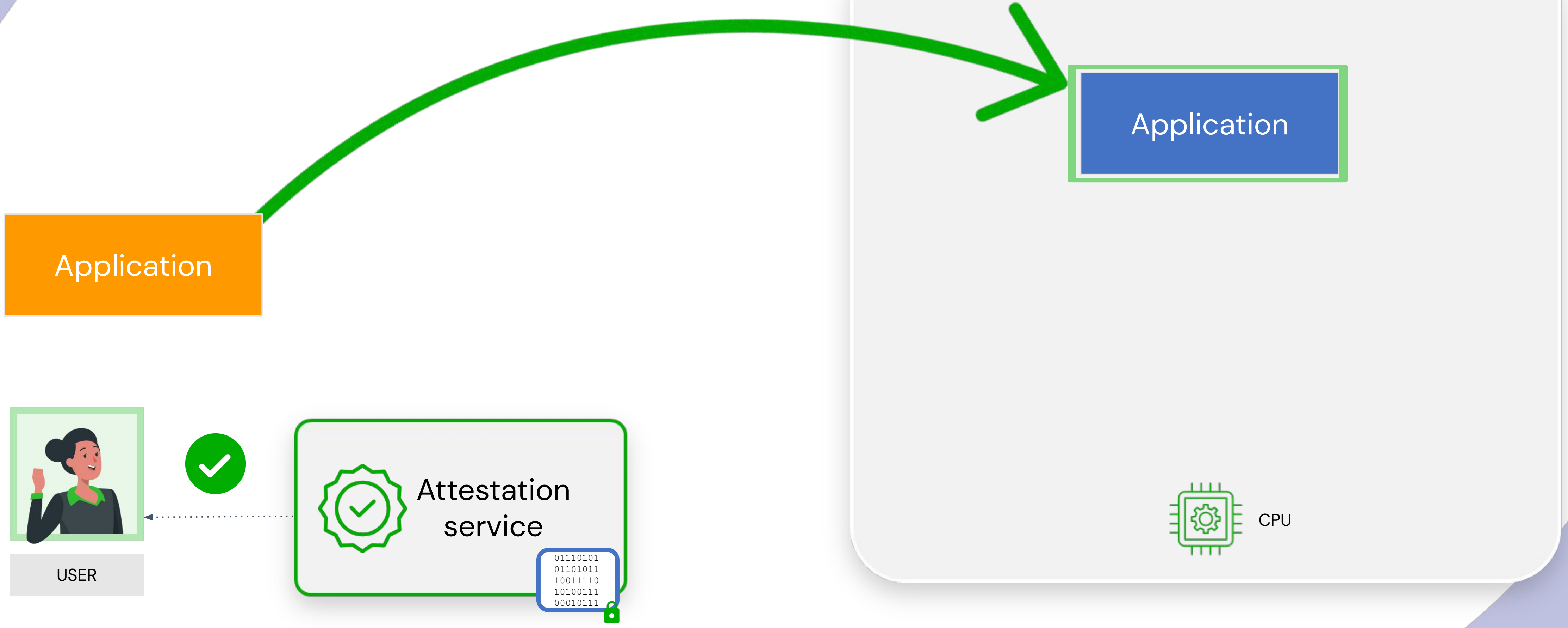
Attestation process



Attestation process



Attestation process



Who needs Confidential Computing?

Who needs Confidential Computing?

(Hint: it’s everyone)

Who needs Confidential Computing?

(Hint: it's everyone)

- Finance, Healthcare, Pharma, Defence, Energy, Government, Telecoms, Enterprise…

Who needs Confidential Computing?

(Hint: it’s everyone)

- Finance, Healthcare, Pharma, Defence, Energy, Government, Telecoms, Enterprise…
- Anyone with
  - Sensitive data
  - Sensitive algorithms

Who needs Confidential Computing?

(Hint: it’s everyone)

- Finance, Healthcare, Pharma, Defence, Energy, Government, Telecoms, Enterprise…
- Anyone with
  - Sensitive data
  - Sensitive algorithms
- In the public Cloud or the Edge
  - Or even private cloud

Who needs Confidential Computing?

(Hint: it’s everyone)

- Finance, Healthcare, Pharma, Defence, Energy, Government, Telecoms, Enterprise…
- Anyone with
  - Sensitive data
  - Sensitive algorithms
- In the public Cloud or the Edge
  - Or even private cloud

(Yup, everyone)

Why open source?

- Visible
- Auditable
- Not just software
  - Meetings (daily stand-ups)
  - Chat (https://chat.enarx.dev)
  - Design process
  - Community involvement

Why open source?

- Visible
- Auditable
- Not just software
  - Meetings (daily stand-ups)
  - Chat (https://chat.enarx.dev)
  - Design process

If it’s not open source,

… you can have no technical assurances in the code,

… nor any basis to trust any system using it.

Thank you

Mike Bursell

https://www.linkedin.com/in/mikebursell/

OpenUK

Presents

STATE OF OPEN CON™23

In association with

IEEE SA OPEN

Thanks to our sponsors

#stateofopencon #soocon23 #openuk