School of Computer Science & Engineering

Trustworthy Systems Group

Introduction to seL4

Foresight S&SAI Workshop, Jul'26, Berlin

Dr Rob Sison

Senior Research Associate, UNSW Sydney

r.sison@unsw.edu.au

I: What is seL4?

What is seL4?

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.**

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified…**

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified…** (what is *that*?)

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified…** (what is *that*?)

Formal verification:

- applied maths for determining software behaviour

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified…** (what is *that*?)

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified…** (what is *that*?)
(to do *what*?)

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified**
to behave according to spec:

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified**
to behave according to spec:

- not to crash.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified**
to behave according to spec:

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* — the software on a machine that runs in **privileged mode.** (i.e. with access to *everything*)

seL4 is **formally verified**
to behave according to spec:

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

Thus, seL4 is reasonably trusted among the most security conscious.

What is seL4?

seL4 is reasonably trusted among the most security conscious.

What is seL4?

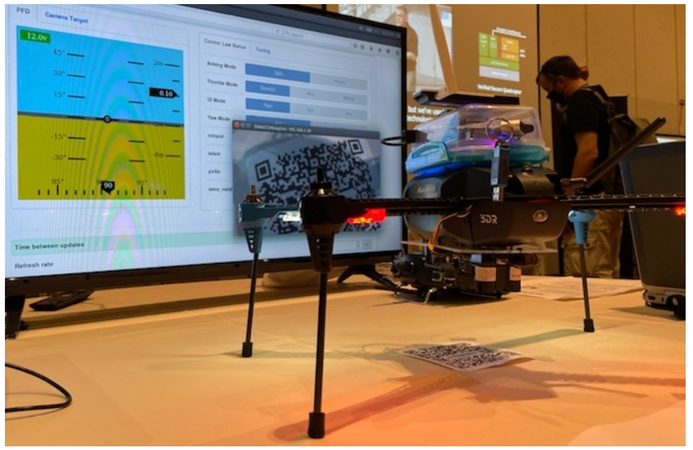
seL4 is reasonably trusted among the most security conscious.

Rockwell Collins put it on a Boeing ULB helicopter and a red team couldn't take control of it. (youtu.be/WAOUbAAGRZs)

What is seL4?

seL4 is reasonably trusted among the most security conscious.

Rockwell Collins put it on a Boeing ULB helicopter and a red team couldn't take control of it. (youtu.be/WAOUbAAGRZs)

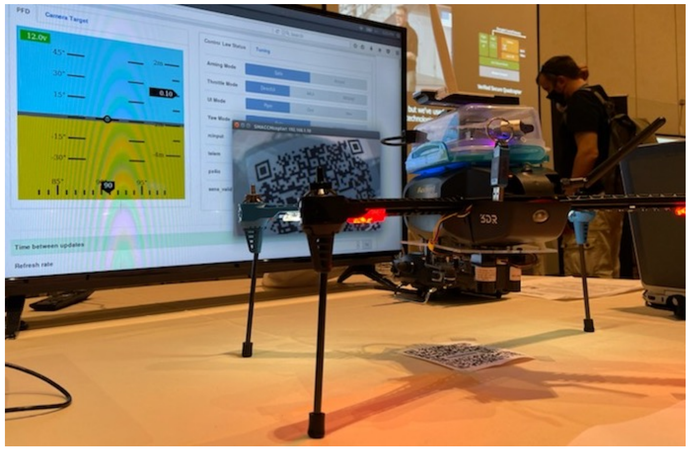


DARPA invited DEF CON attendees to "Steal This Drone" running on seL4, and they couldn't. (loonwerks.com/publications/cofer2021defcon.html)

What is seL4?

seL4 is reasonably trusted among the most security conscious.

Rockwell Collins put it on a Boeing ULB helicopter and a red team couldn't take control of it. (youtu.be/WAOUbAAGRZs)



DARPA invited DEF CON attendees to "Steal This Drone" running on seL4, and they couldn't. (loonwerks.com/publications/cofer2021defcon.html)

Neutrality is using it to develop cloud services vs oppressive nation-state actors. (neutrality.ch/about/)

What is seL4?

seL4 is an *OS kernel* that's **formally verified**

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* that's **formally verified**

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

What is seL4?

seL4 is an *OS kernel* that's **formally verified**

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

seL4 is a *platform for OS & verification research* on

What is seL4?

seL4 is an *OS kernel* that's **formally verified**

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

seL4 is a *platform for OS & verification research* on

- proving other security outcomes.
  (e.g. time protection, trustworthy.systems/projects/timeprotection)

Thanks to funding from

cyberagentur

What is seL4?

seL4 is an *OS kernel* that's **formally verified**

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

seL4 is a *platform for OS & verification research* on

- proving other security outcomes.
  (e.g. time protection, trustworthy.systems/projects/timeprotection)
- verifying more than just the OS kernel.
  (e.g. userland OS components, trustworthy.systems/projects/compositionality

Thanks to funding from

cyberagentur

What is seL4?

seL4 is an *OS kernel* that's **formally verified**

- not to crash.
- to enforce some security outcomes.

Formal verification:

- applied maths for determining software behaviour
- e.g. proofs by induction over software structure

seL4 is a *platform for OS & verification research* on

- proving other security outcomes.
  (e.g. time protection, trustworthy.systems/projects/timeprotection)
- verifying more than just the OS kernel.
  (e.g. userland OS components, trustworthy.systems/projects/compositionality
  … and that seL4 meets their needs, trustworthy.systems/projects/kugap)

Thanks to funding from

cyberagentur

FORESIGHT INSTITUTE

II: Trust, seL4 and AI

Trust, seL4 and AI

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

- AI's value is in its *unpredictability*.

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

- AI's value is in its *unpredictability*.
- OS kernels are where you **do not** want unpredictable things to happen.

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

- AI's value is in its *unpredictability*.
- OS kernels are where you **do not** want unpredictable things to happen.

Questions as an AI outsider:

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

- AI's value is in its *unpredictability*.
- OS kernels are where you **do not** want unpredictable things to happen.

Questions as an AI outsider:

- What is the state of the art in thinking on privacy and security with AI?

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

- AI's value is in its *unpredictability*.
- OS kernels are where you **do not** want unpredictable things to happen.

Questions as an AI outsider:

- What is the state of the art in thinking on privacy and security with AI?
- Where are the potential roles for AI in trusted OS settings?

Trust, seL4 and AI

Many people trust seL4, an OS kernel that's formally verified.

- Trust is based on *predictability.*
- Formal verification is a **means** of ensuring predictability.

Things I regard to be common sense:

- AI's value is in its *unpredictability*.
- OS kernels are where you **do not** want unpredictable things to happen.

Questions as an AI outsider:

- What is the state of the art in thinking on privacy and security with AI?
- Where are the potential roles for AI in trusted OS settings?
- What should the basis be for our trust in AI?