May 5, 2025

Max Taylor
Formal Methods Researcher

Automated Reasoning for UAV Safety & Security

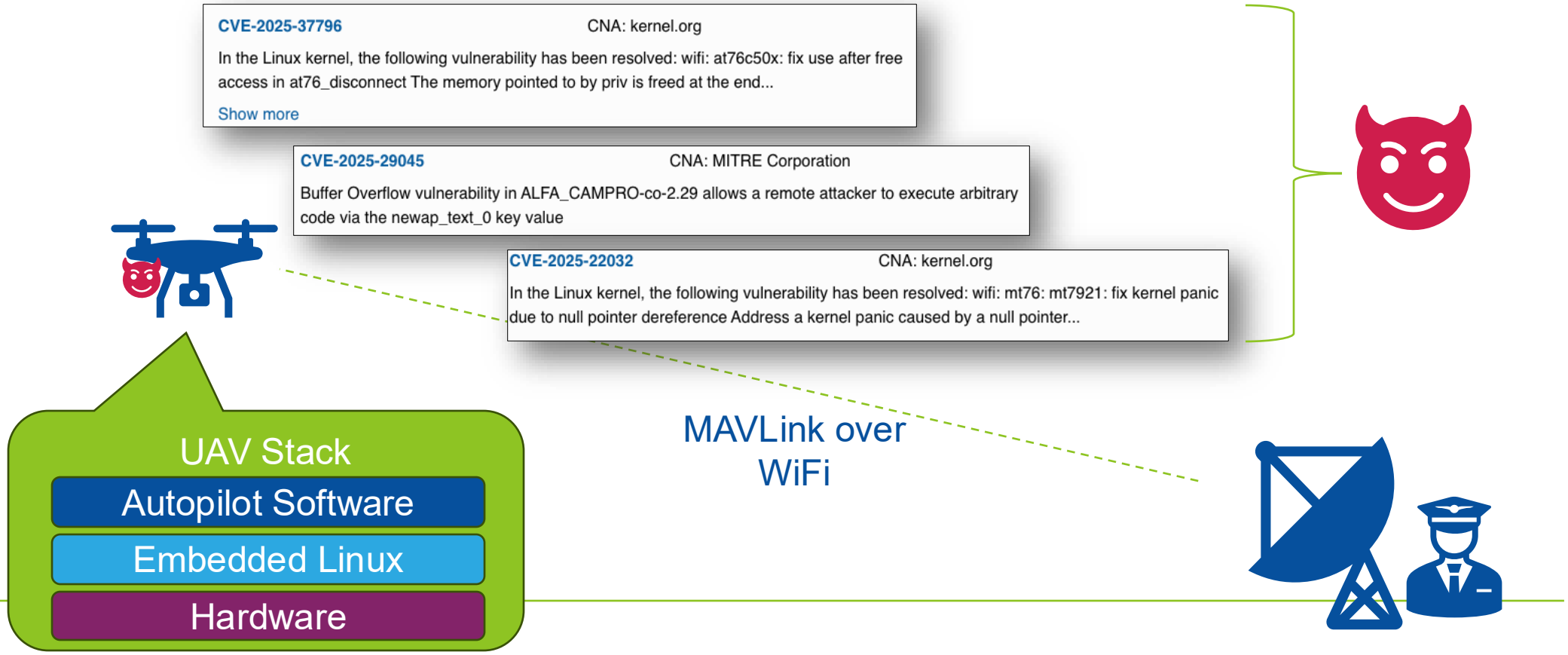
The Datum Protocol Stack

Arthur Amorim, Max Taylor, Gary T. Leavens, William L. Harrison, Lance Joneckis, and Trevor Kann

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

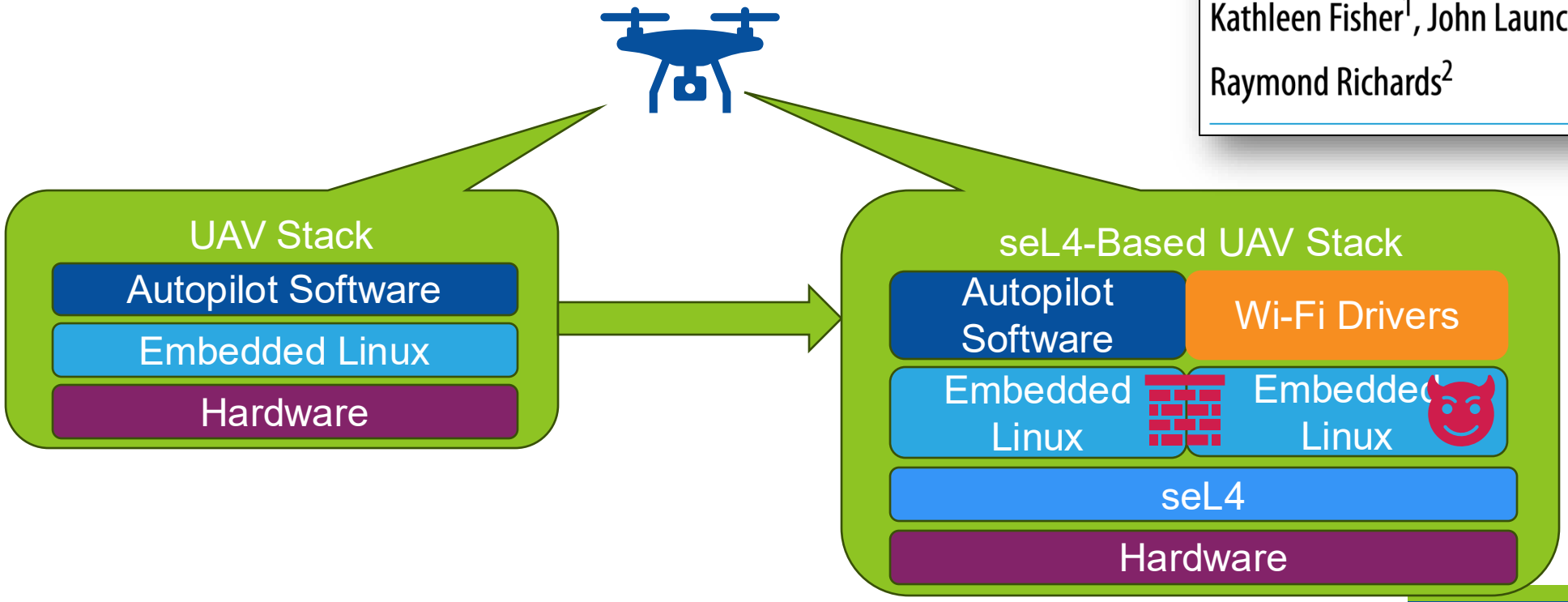
seL4-based architectures help protect UAVs against sophisticated adversaries



seL4-based architectures help protect UAVs against sophisticated adversaries

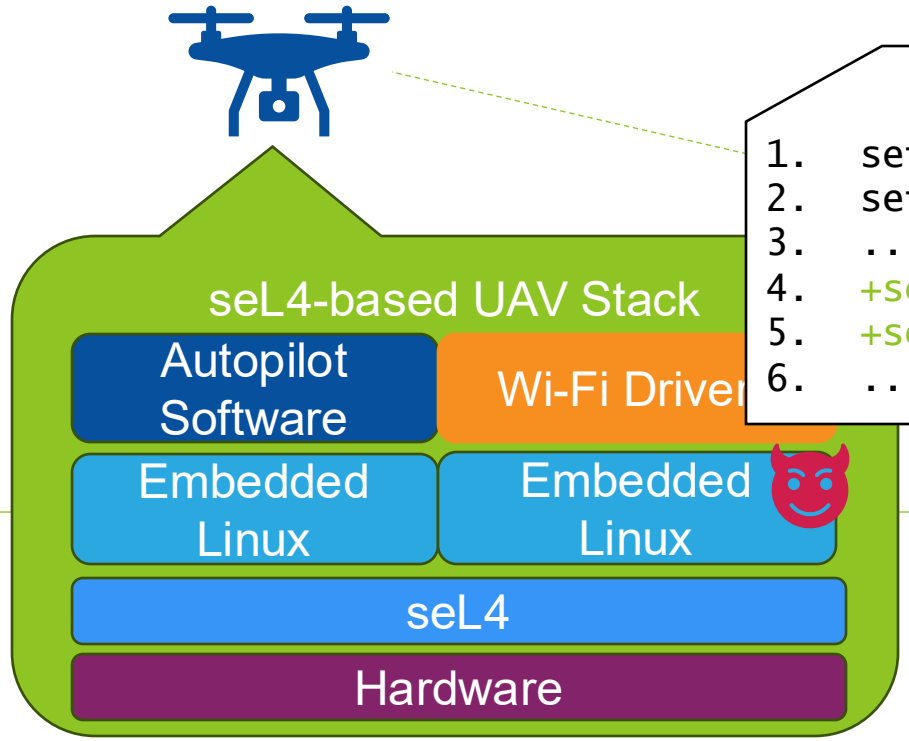
The HACMS program: using formal methods to eliminate exploitable bugs

Kathleen Fisher[1], John Launchbury[2,†] and Raymond Richards[2]



However, sophisticated adversaries can launch *stealthy attacks*

Stealthy attacks occur when an adversary manipulates a system to compromise its functionality while evading detection




```
1.  set TAKEOFF_ALT 20
2.  set FLIGHT_MIN_ALT 10
3.  ...
4.  +set PITCH_GAIN_P MAX
5.  +set PITCH_GAIN_FF_P MAX
6.  ...
```

RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles Through Control-Guided Testing

Taegyu Kim†, Chung Hwan Kim*, Junghwan Rhee*, Fan Fei†, Zhan Tu†, Gregory Walkup†
Xiangyu Zhang†, Xinyan Deng†, Dongyan Xu†
†*Purdue University, {tgkim, feif, tu17, gwalkup, xyzhang, xdeng, dxu}@purdue.edu*
**NEC Laboratories America, {chungkim, rhee}@nec-labs.com*

We prevent stealthy attacks using Datum by writing protocols that preclude undesirable system behaviors

Dynamically **A**ssured **T**yped **U**niversal **M**essaging (DATUM) is our framework for building high-assurance systems rooted in well-defined protocols

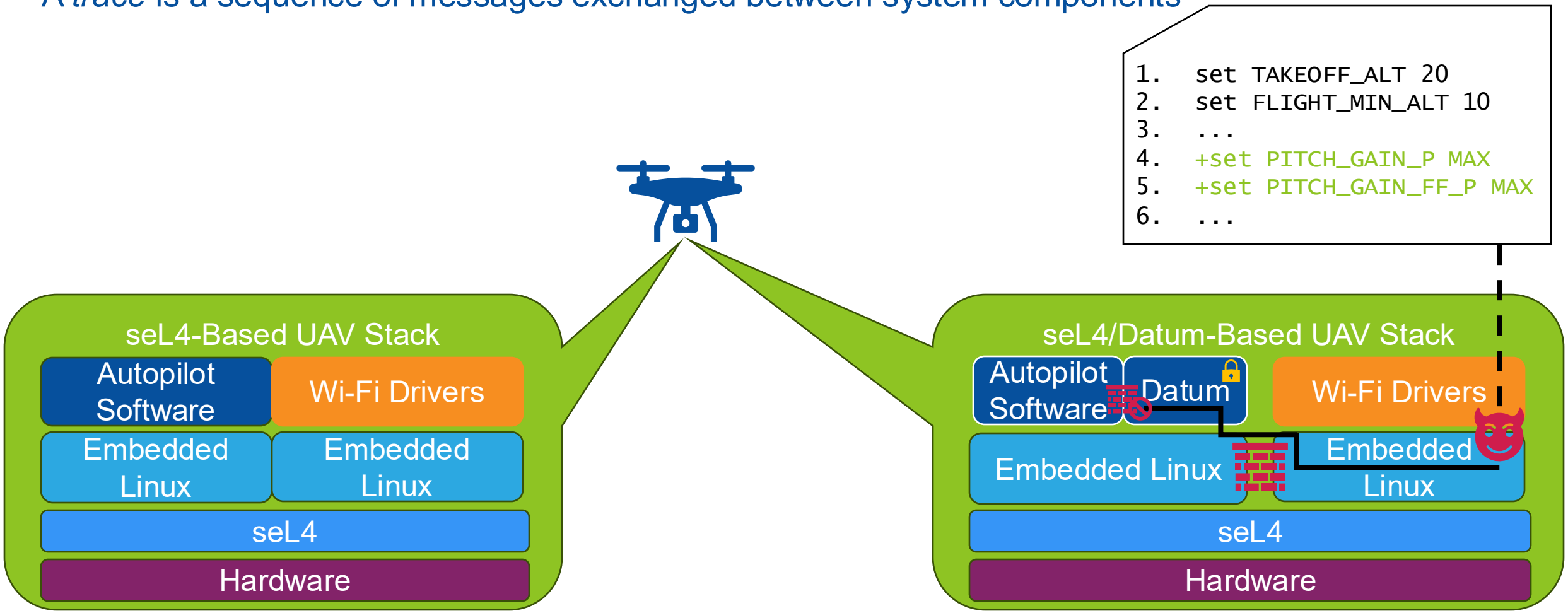
```
1. set TAKEOFF_ALT 20
2. set FLIGHT_MIN_ALT 10
3. ...
4. +set PITCH_GAIN_P MAX
5. +set PITCH_GAIN_FF_P MAX
6. ...
```

```
PITCH_GAIN_P + PITCH_GAIN_FF_P < T
```

Datum Protocol

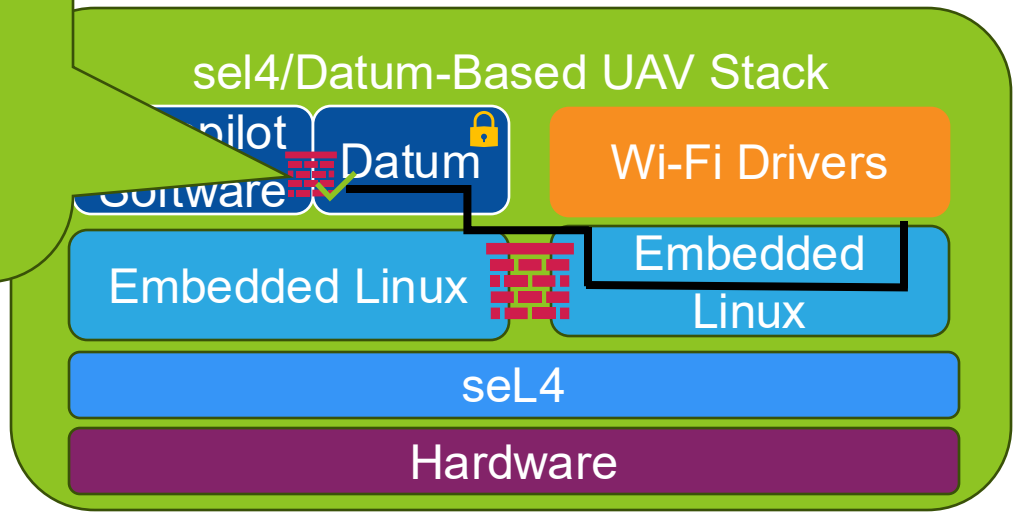
Datum enforces protocols by dynamically checking *traces*

A *trace* is a sequence of messages exchanged between system components

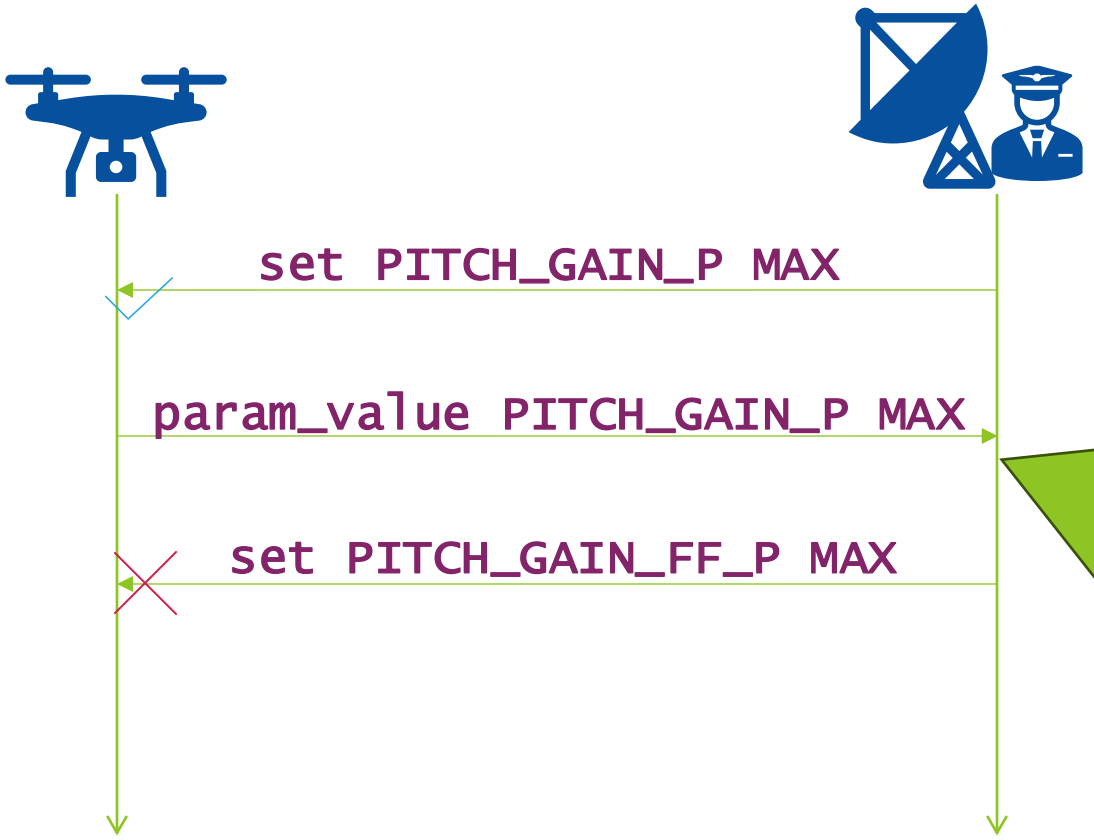


Traces that conform to a protocol maintain safety invariants

```
trace_conforms tr proto
⇒
control_stability tr
```



Datum represents protocols using *Refined Multiparty Session Types (RMPSTs)*



1. Permissible messages
2. Message order
3. Message contents

Statically Enforced!

Statically Verified Refinements for Multiparty Protocols

FANGYI ZHOU, Imperial College London, United Kingdom
FRANCISCO FERREIRA, Imperial College London, United Kingdom
RAYMOND HU, University of Hertfordshire, United Kingdom
RUMYANA NEYKOVA, Brunel University London, United Kingdom
NOBUKO YOSHIDA, Imperial College London, United Kingdom

```
1. μ (λ (_ : unit) ->
2.  Choice UAV GCS [
3.   option "set"
4.    (λ (p : hidden param_set_msg) ->
5.      Choice GCS UAV [
6.       option "param_value"
7.        (λ (p : hidden param_val_msg) ->
8.          Recur 0 ())])])
```

Datum embeds RMPSTs in the F* interactive theorem prover (ITP)

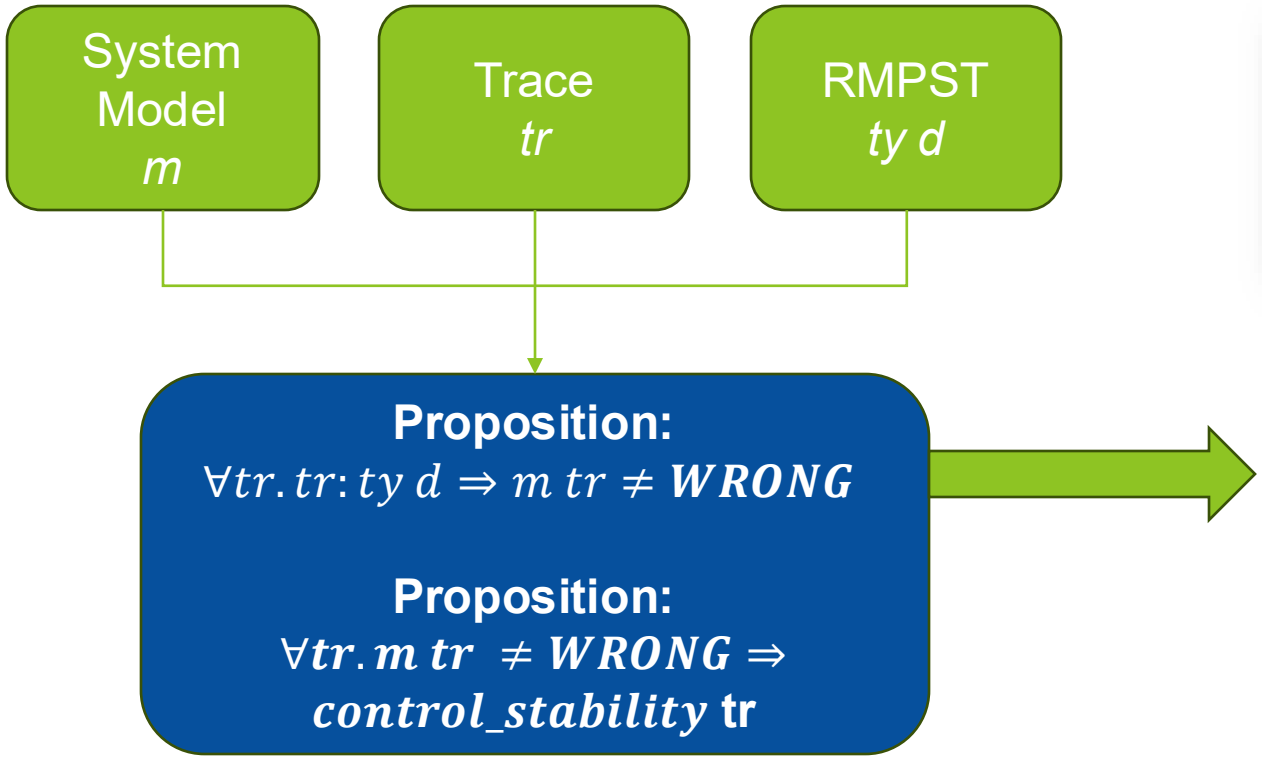
```
unfold type proto_val (#u : Type) (ty : session_type u) = H.hidden (stamped_val ty)

noeq type global_session (u : Type) : (#nparticipants : ℕ) → (#l : list label) → (rec_contexts : list (session_type u)) → (k : global_session_kind) → Type =
  | Choice :  (#npa        ipants : ℕ) →
              (#rec_co           (session_type u)) →
              (from : ℕ                    }) →
              (to : ℕ { to
                                                          _labels l}) →
  | Mu
  | Rec
  | End :
```

```
let m2'' = Choice alice bob [
  mkoption "foo"
           (λ (x : proto_val (RefType (λ (x : (prim_val unit StampInt)) → H.return (even (Int?.v x))))) →
             (Mu (RefType (λ (x : (prim_val unit StampInt)) → (H.return (odd (Int?.v x)))))
               (H.lift (λ x' → (Val (Int ((Int?.v (Val?.v x')) + 1)))) x)
               (λ _ → End)));
]
```


IDAHO NATIONAL LABORATORY

Datum's F*-based representation enables machine-checked proofs of key protocol safety properties

Proposition: Well-typed traces don't go wrong



Towards Provable Security in Industrial Control Systems Via Dynamic Protocol Attestation

Arthur Amorim, *University of Central Florida, Florida, USA*, *arthur.amorim@ucf.edu*
Trevor Kann, *Carnegie Mellon University, Pittsburgh, USA*, *tkann@cmu.edu*
Max Taylor, *Idaho National Laboratory, Idaho Falls, USA*, *maxwell.taylor@inl.gov*
Lance Joneckis, *Idaho National Laboratory, Idaho Falls, USA*, *lance.joneckis@inl.gov*

[ICSS '24]

Provably Safe Protocol:
sRMPST

F*'s programming facilities enables Datum to generate dynamic attestors

Enforcing MAVLink Safety & Security Properties Via Refined Multiparty Session Types

Arthur Amorim[1][0009−0003−7712−5055], Max Taylor[2][0009−0005−7873−9694], Trevor Kann[3][0009−0004−5197−2448], William L. Harrison[2][0000−0002−3760−3556], Gary T. Leavens[1][0000−0003−3271−3921], and Lance Joneckis[2][0009−0002−0284−4787]

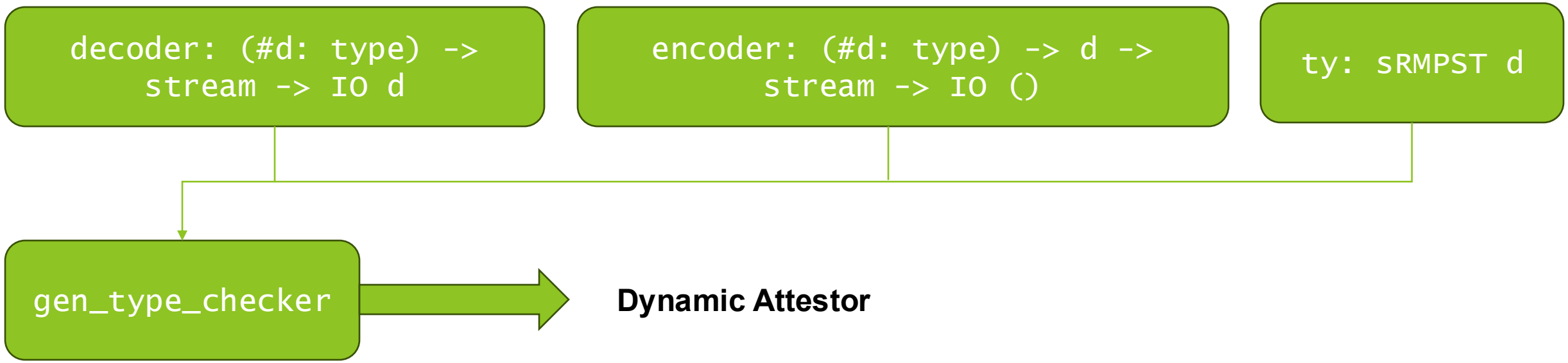
Linux-Based Integration
[NASA FM '25]

UAV Resilience Against Stealthy Attacks

Arthur Amorim*, Max Taylor†, Trevor Kann‡, Gary T. Leavens*, William L. Harrison†, and Lance Joneckis†

seL4-Based Integration
[ICUAS '25]

Datum's dynamic attestors are extendable to additional transports using a well-defined interface



Datum enables formal protocol descriptions

- Protocols are expressed as Refined Multiparty Session Types (RMPSTs)
  - This choice allows us to statically verify programs implement a protocol
- Our future work will build on previous efforts that have integrated vanilla session types with systems programming languages

Session Types for Rust

Thomas Bracht Laumann Jespersen Philip Munksgaard Ken Friis Larsen

Department of Computer Science, University of Copenhagen, Denmark

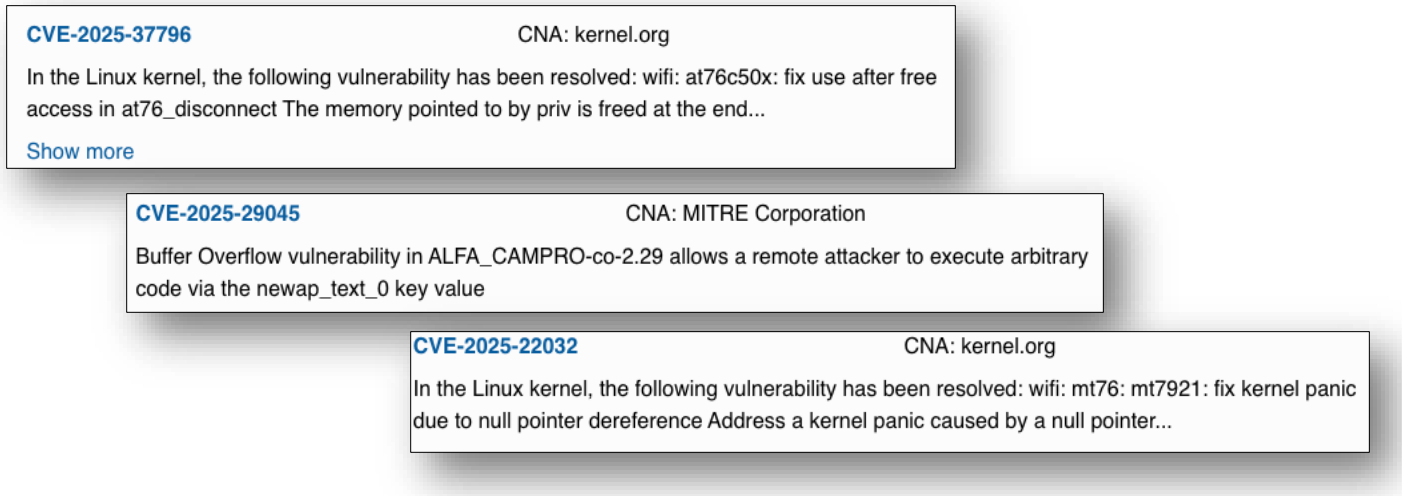
ntl316@alumni.ku.dk pmunksgaard@gmail.com kflarsen@diku.dk

A Concept and Template Meta-programming Approach to Session Types in C++

Protocols developed using Datum can be shown to preserve critical invariants

- The behavior of the system after receiving a message is described by a model
  - The model goes *wrong* if the system's next state violates an invariant
- We can prove that if a trace conforms to a protocol, then interpreting the trace does not cause the system to go *wrong* (i.e., well-typed traces don't go wrong)

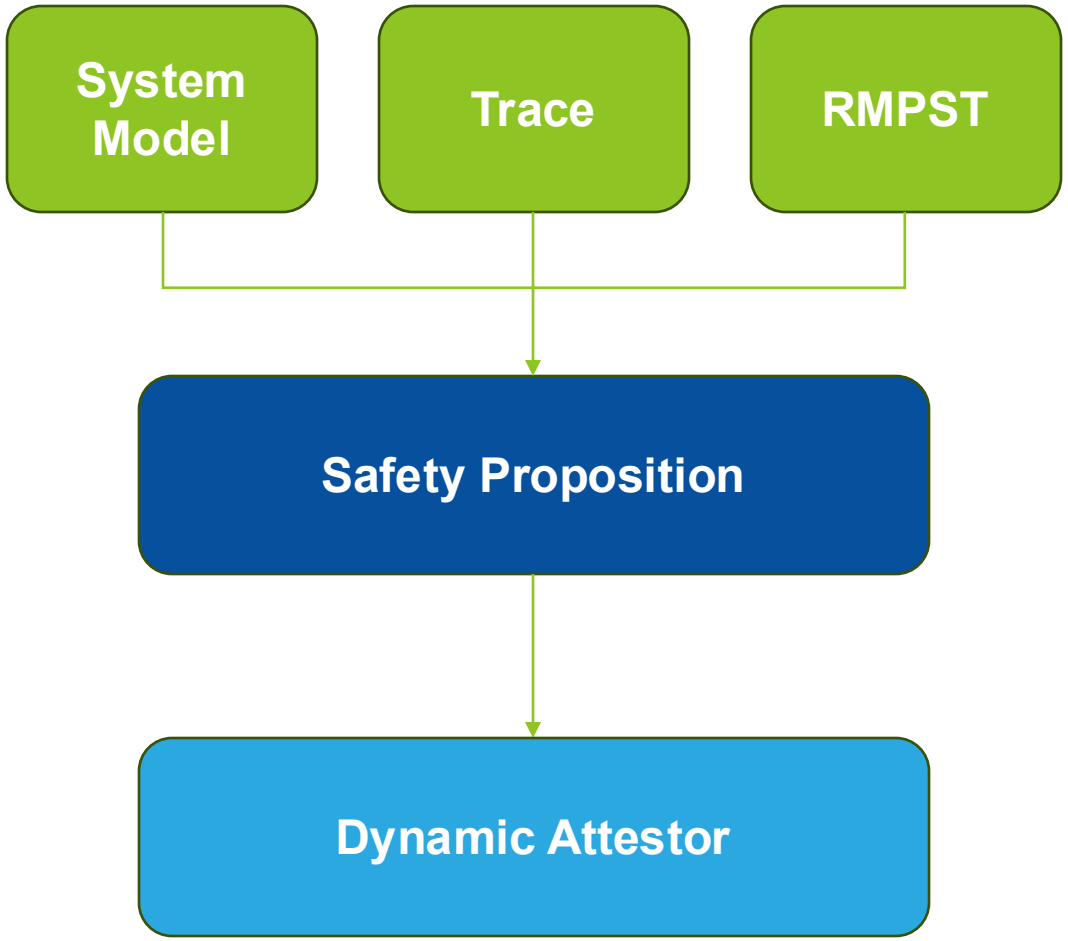
Preserving these invariants + seL4 integration eliminates entire categories of attacks



Exploiting these vulnerabilities does not compromise UAV's safety!

Questions?

The Datum Protocol Framework



Slides

Max Taylor
Formal Methods Researcher
Idaho National Laboratory
maxhtaylor@proton.me

Dynamic Attestor Pipeline

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.