ICUAS

UAV Resilience Against Stealthy Attacks

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

We show how to leverage runtime monitoring and high-assurance operating systems to defend against sophisticated adversaries.

INL Idaho National Laboratory

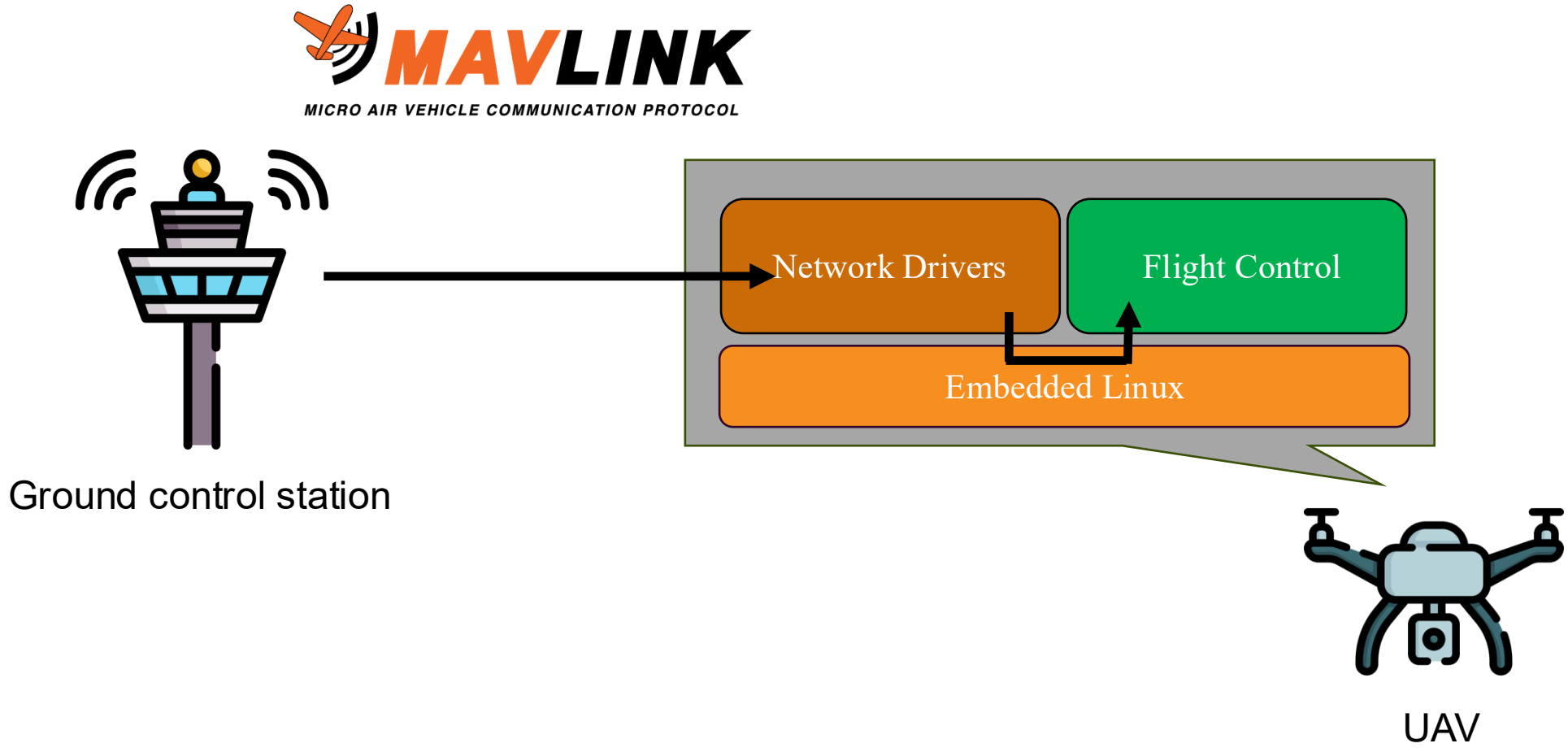
UAVs are desirable targets for adversaries because they depend on untrusted software components to automate critical missions.

Military Operations

Search and Rescue

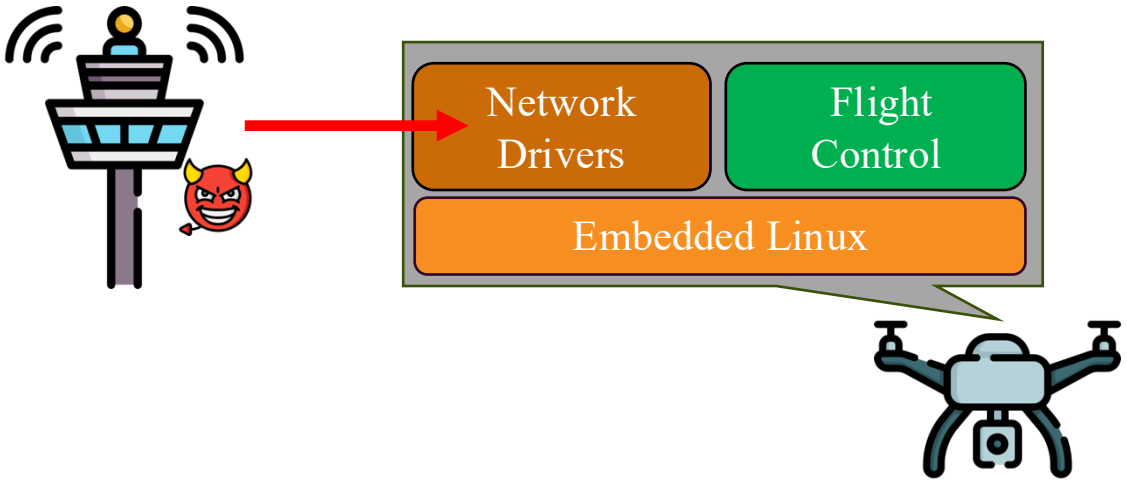
Disaster Response

UAVs rely on a complex software stack that significantly expands the attack surface.

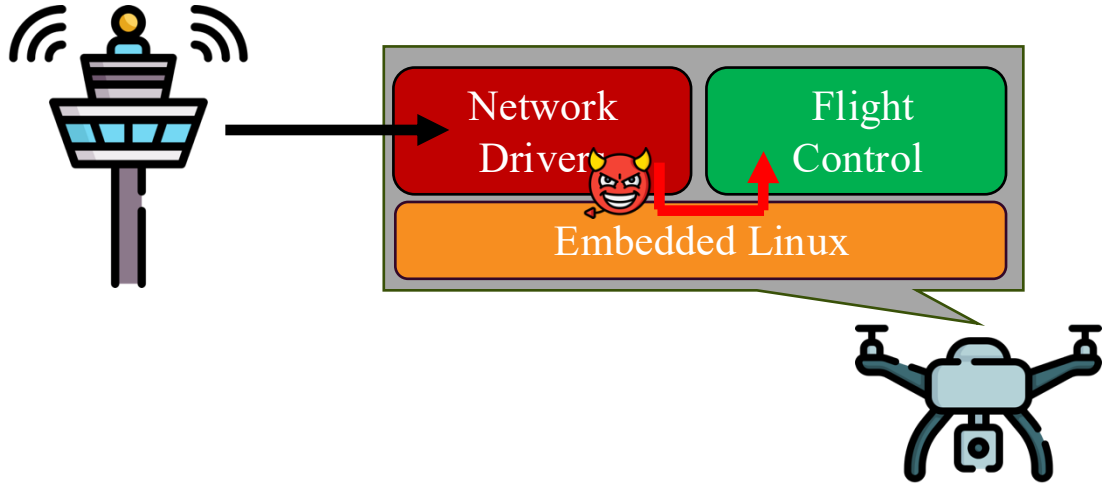


In this work we consider two attack models and combine UAV resiliency approaches into an architecture that protects against both.

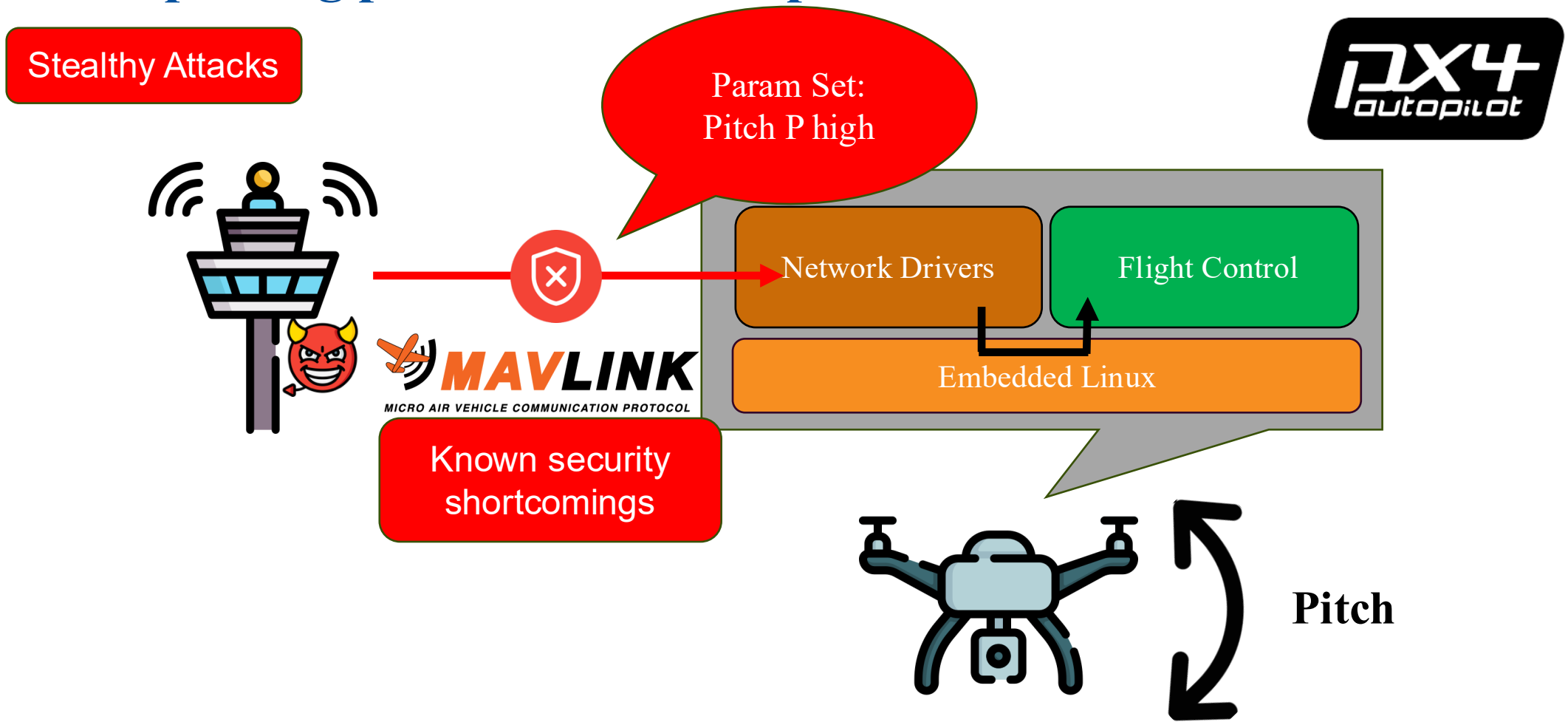
Stealthy Attacks



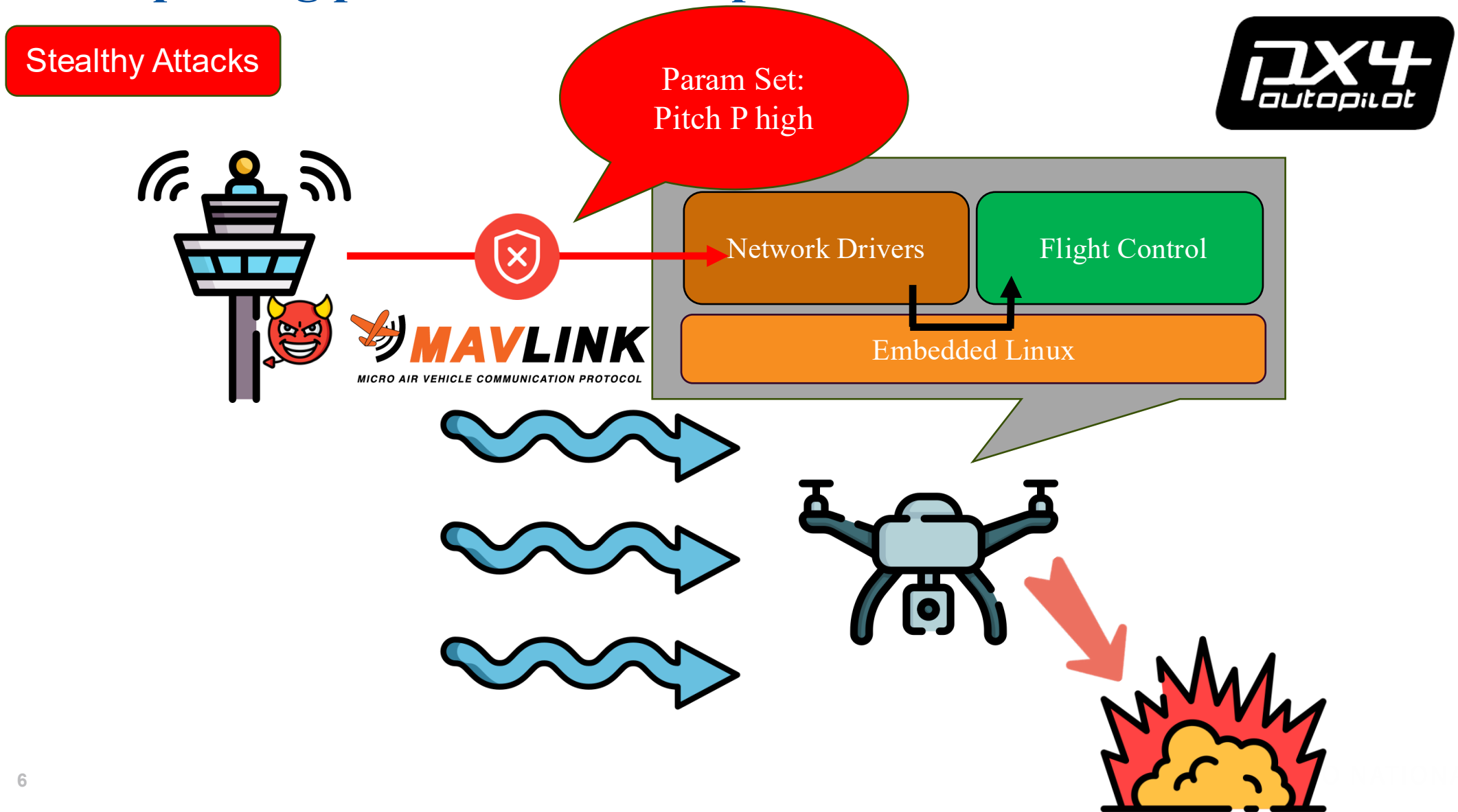
Driver Attacks



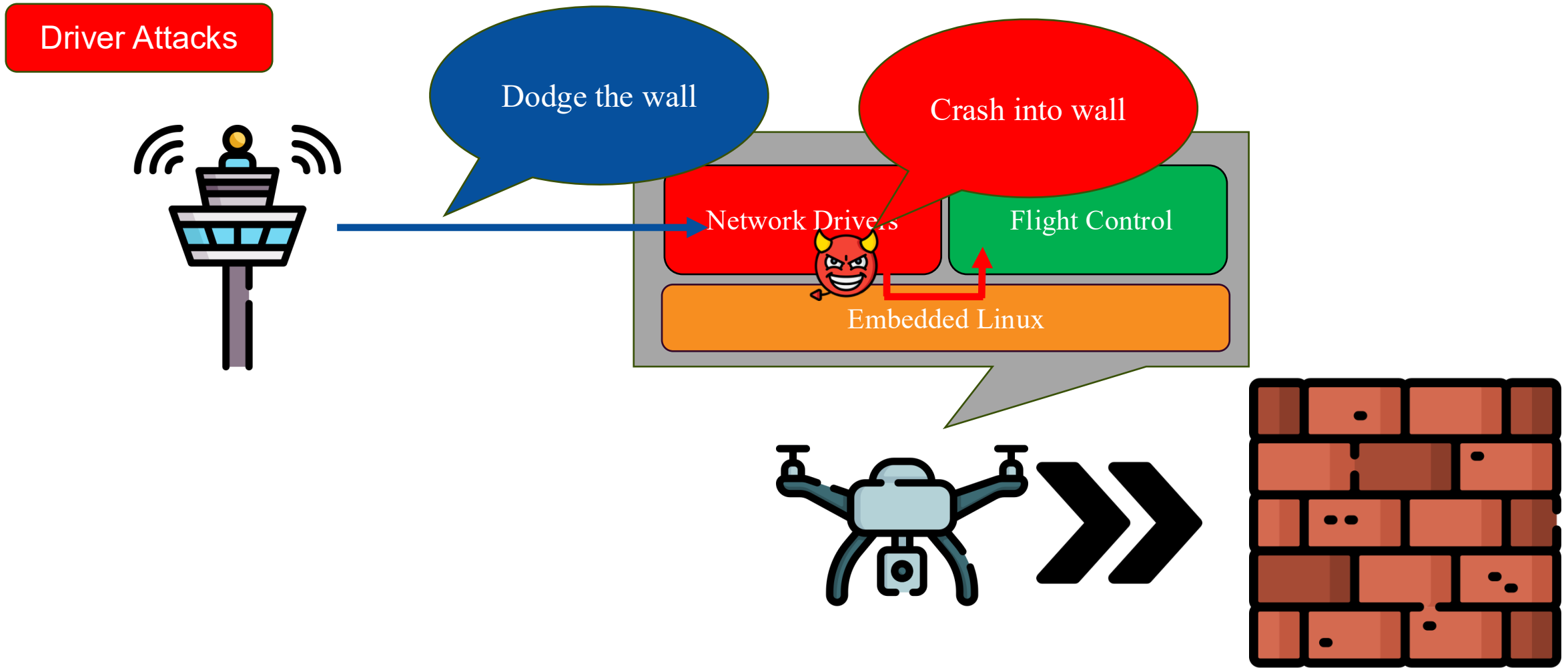
A compromised ground control station can launch stealthy attacks by exploiting parameter interdependencies.



A compromised ground control station can launch stealthy attacks by exploiting parameter interdependencies.

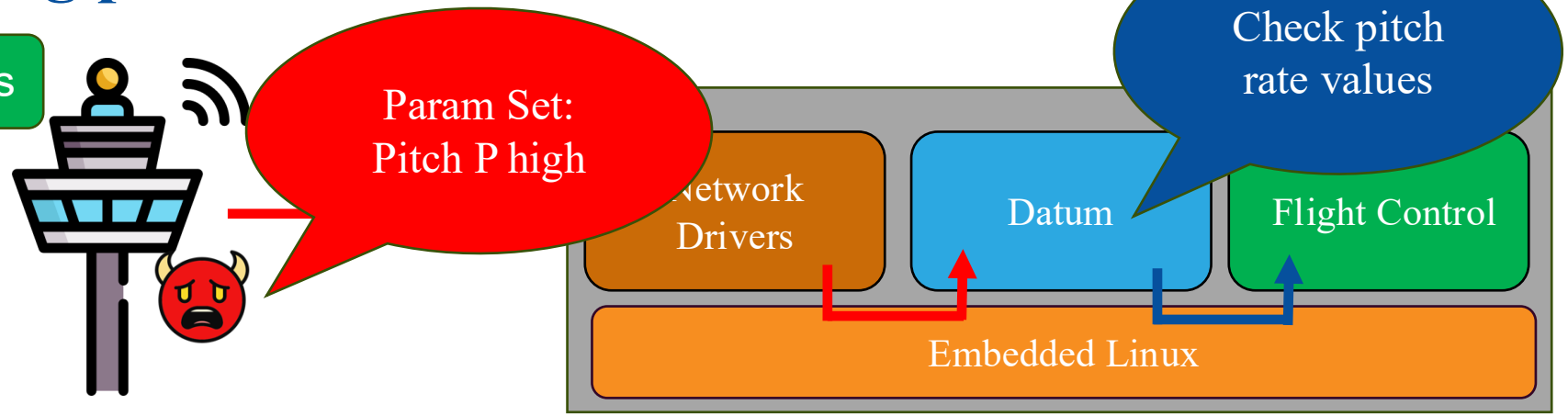


A compromised UAV driver can override mission safety checks and induce dangerous behavior.



Datum can detect and prevent stealthy attacks at runtime by enforcing parameter-level constraints.

Stealthy Attacks



Datum Framework

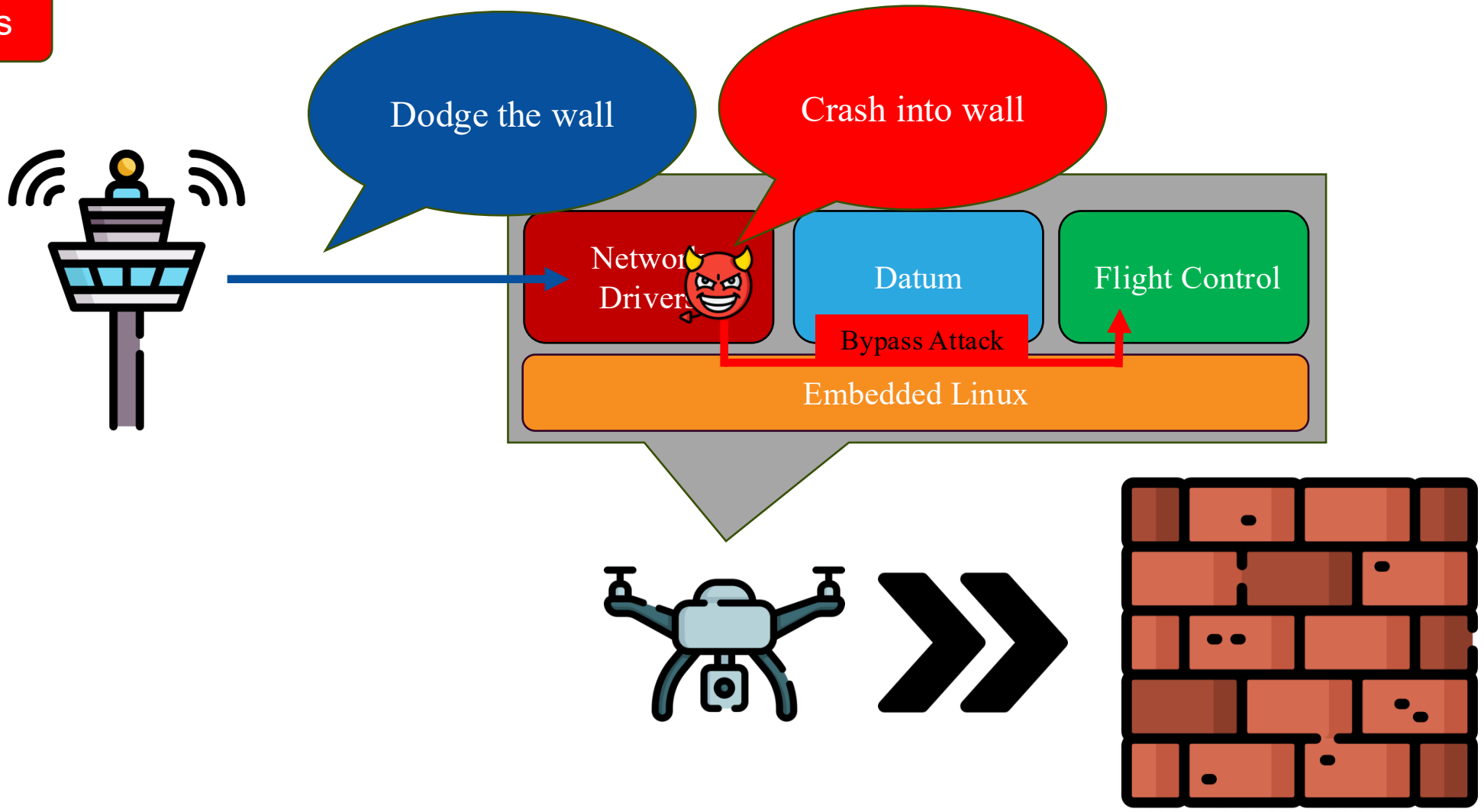
1- Extract existing protocol

2- Add constraints to messages

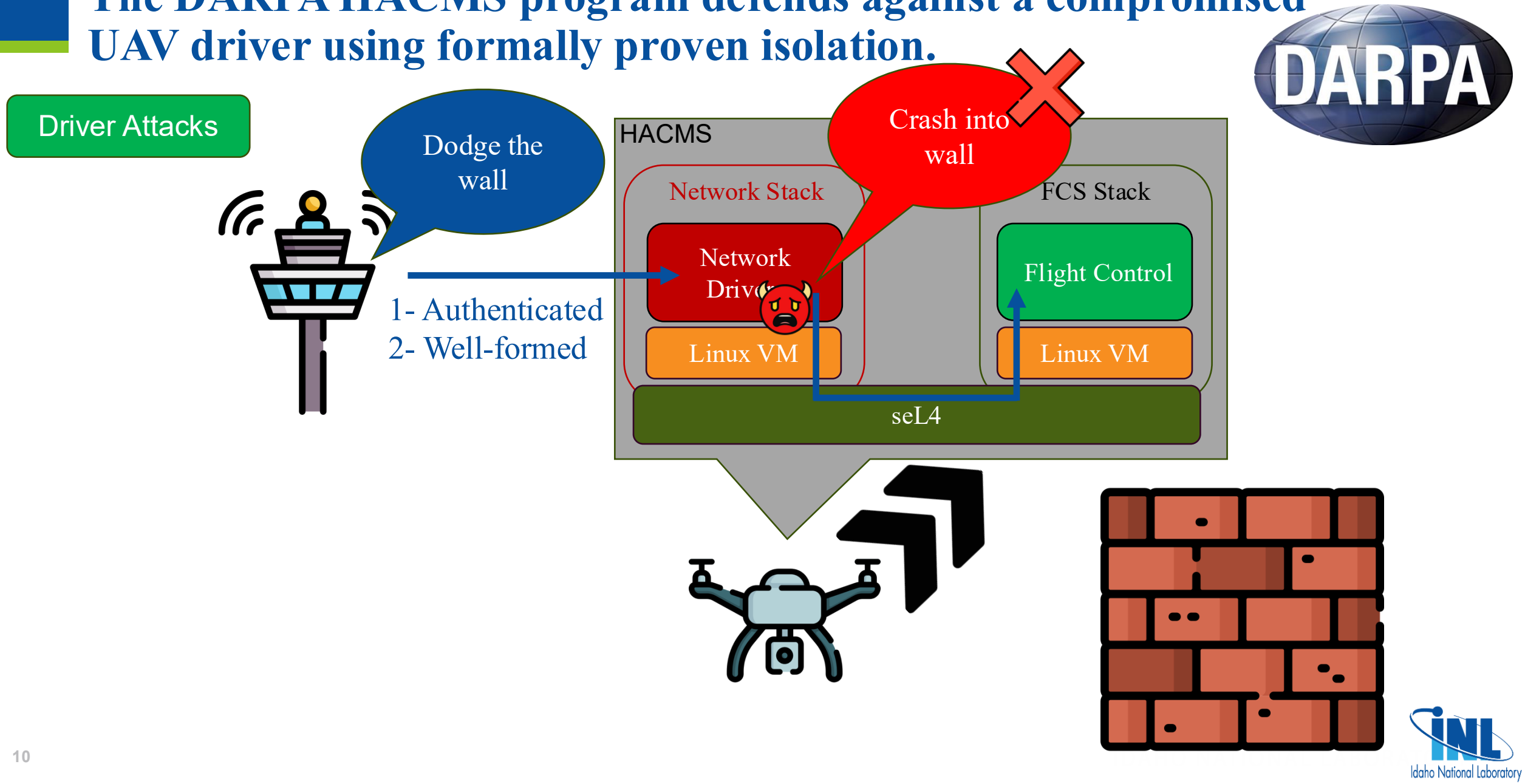
3- Runtime checking

However, Datum is ineffective against driver attacks that bypass its checks.

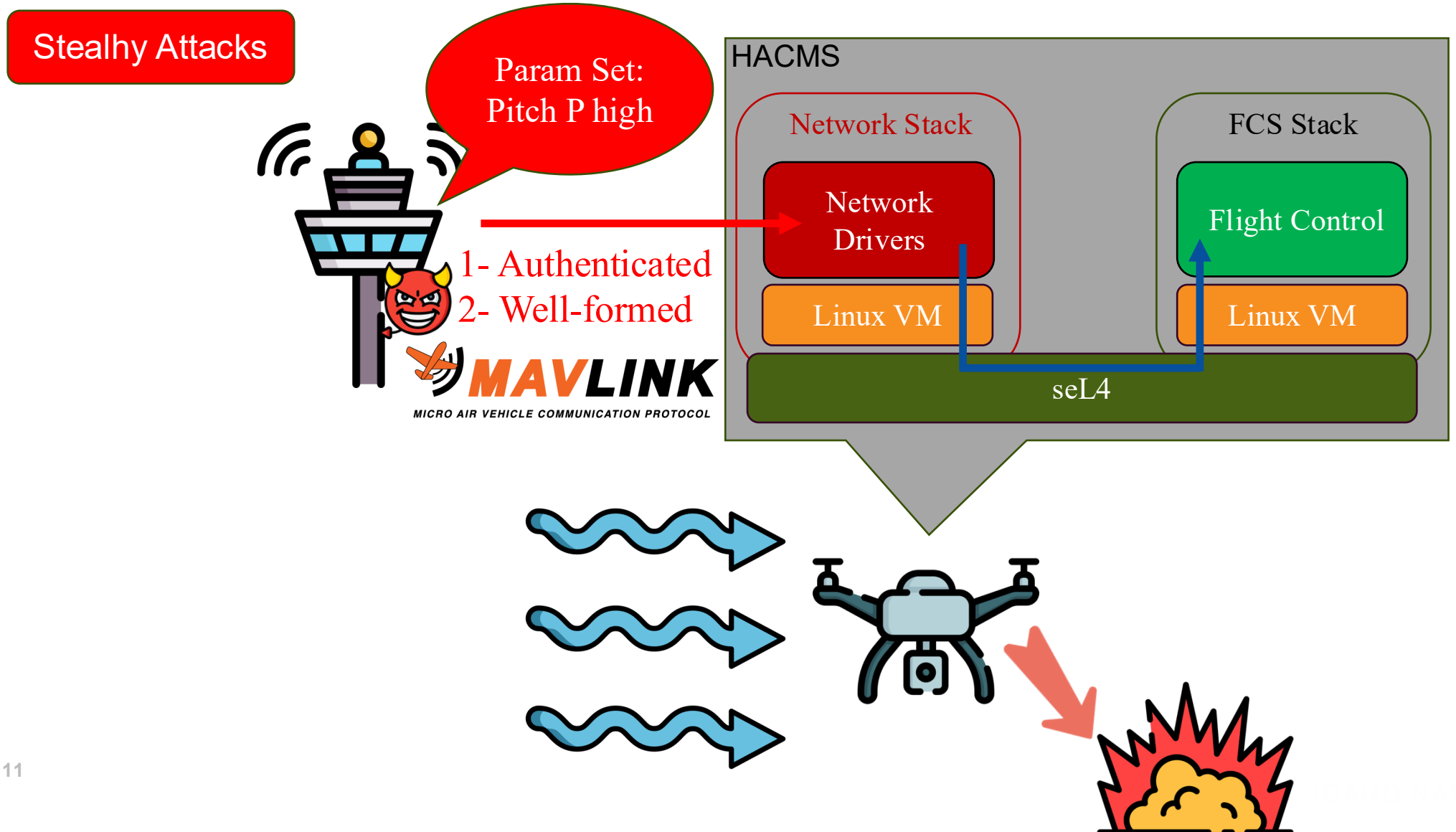
Driver Attacks



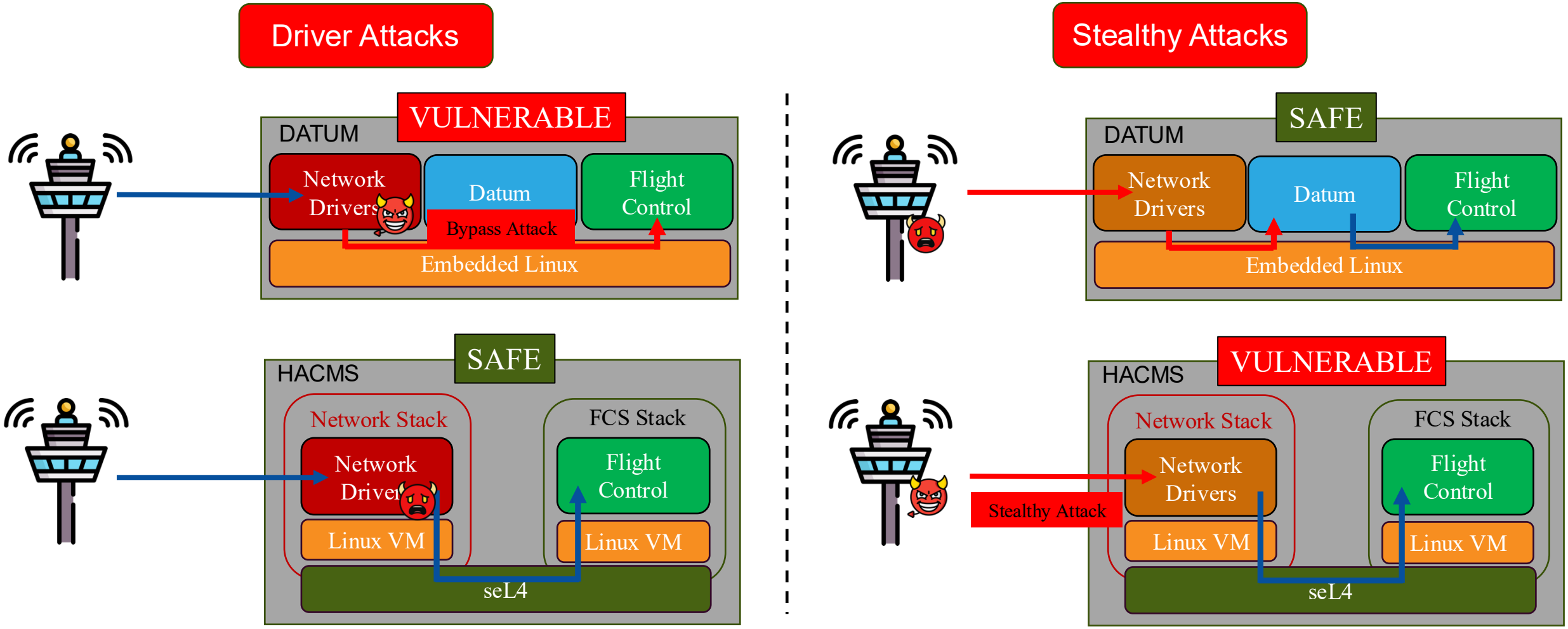
The DARPA HACMS program defends against a compromised UAV driver using formally proven isolation.



However, stealthy attacks from a compromised ground control station remain effective, even against HACMS-style architectures.

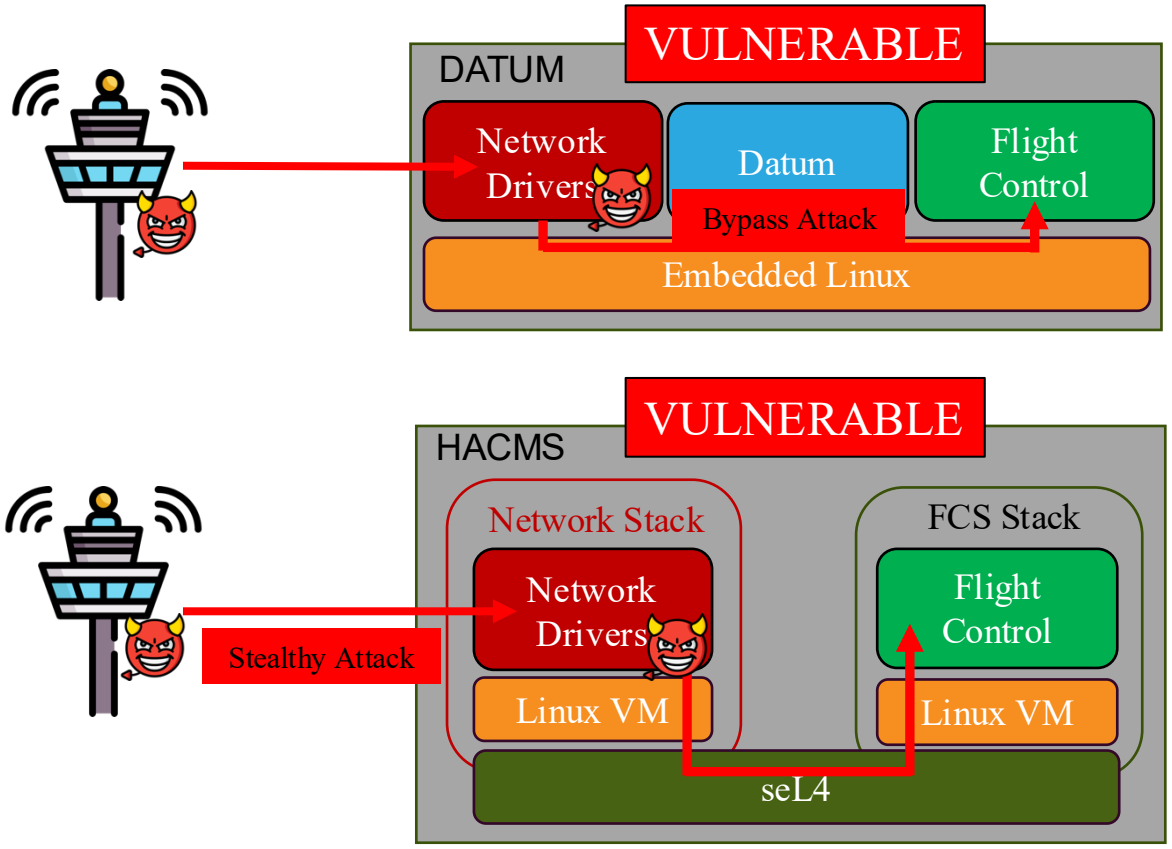


HACMS and Datum prevent only one of the attacks, while being vulnerable to the other.



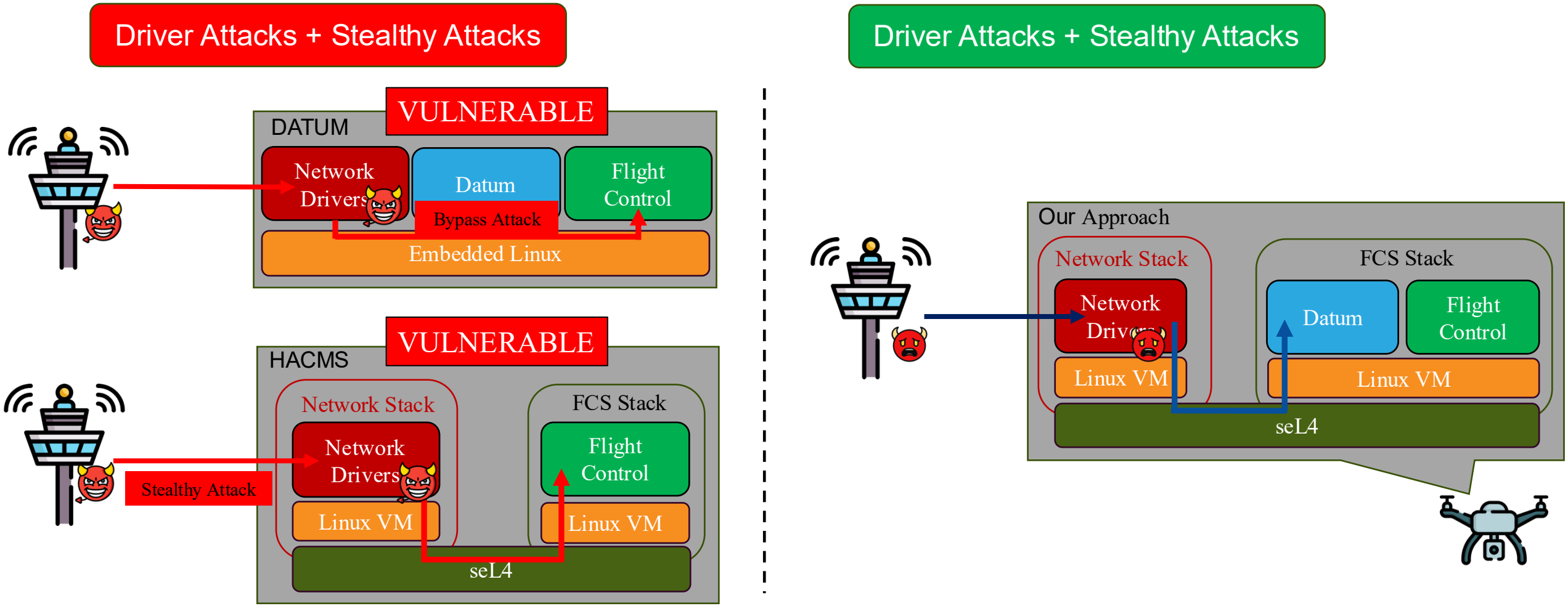
A resourceful attacker who compromises both the ground control station and a UAV driver can sabotage both approaches.

Driver Attacks + Stealthy Attacks



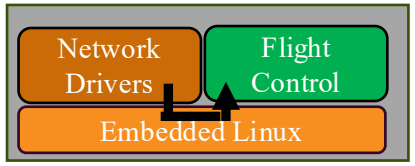
Attack Model: An attacker has compromised both the GCS and a UAV driver.

Our system composes HACMS and Datum in a single architecture to defend against this powerful adversary.

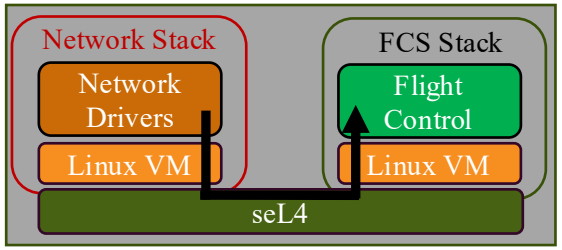


The evaluation shows our architecture adds acceptable overhead.

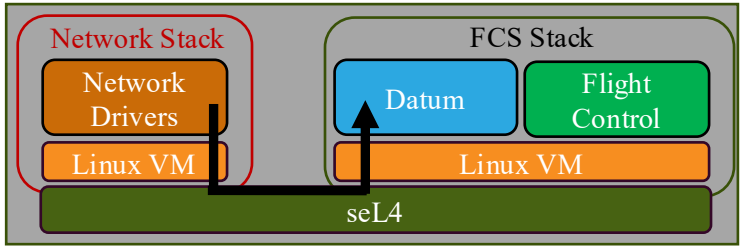
1- Baseline

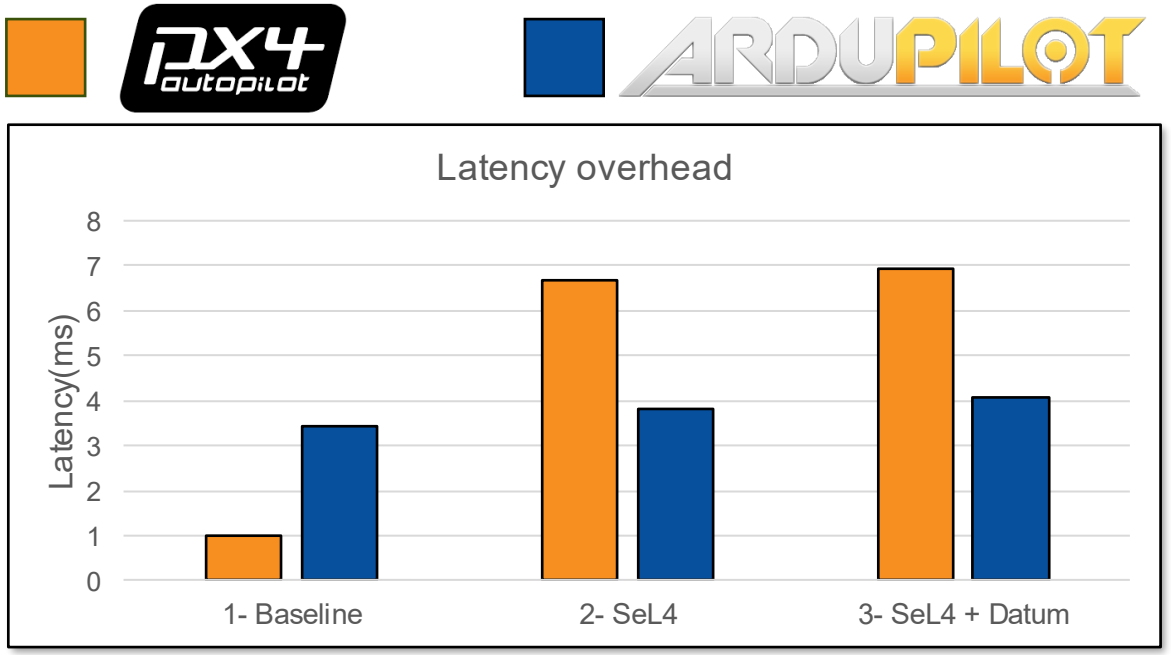


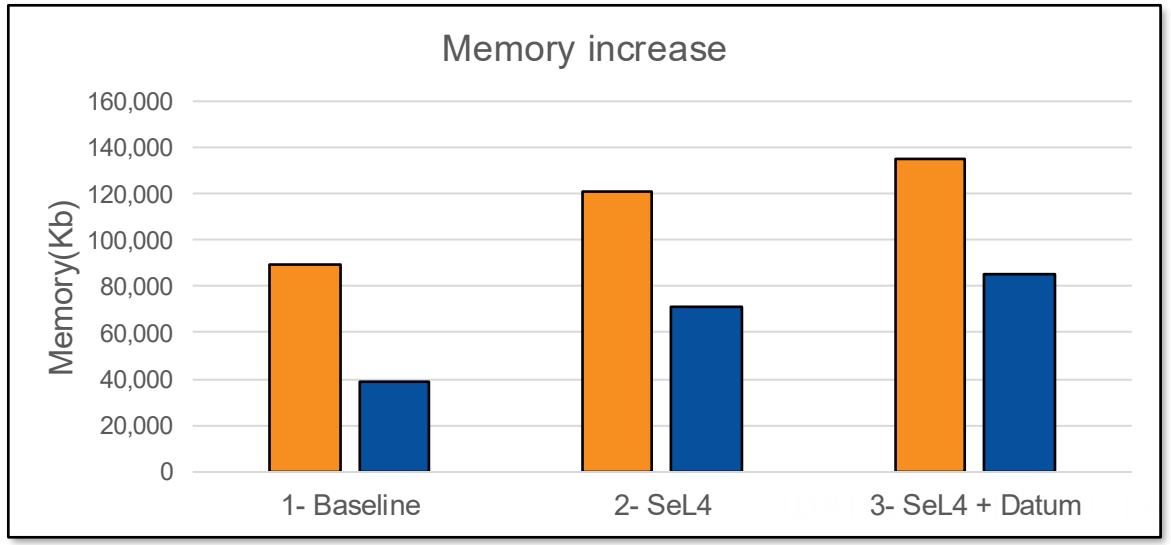
2- seL4



3- seL4 + Datum



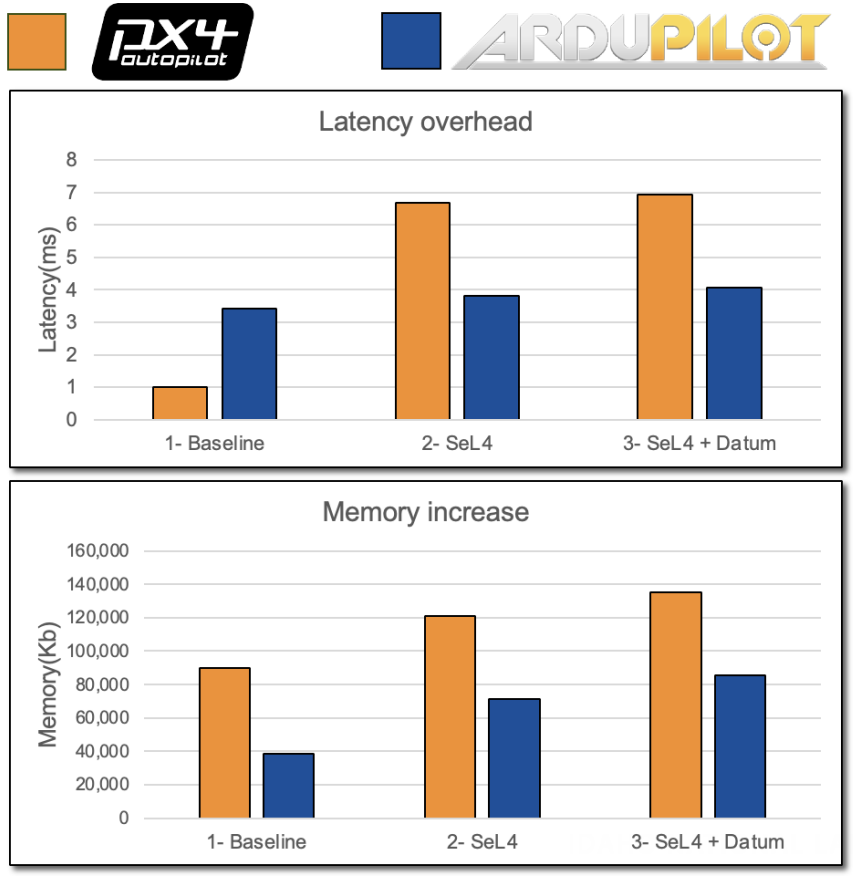


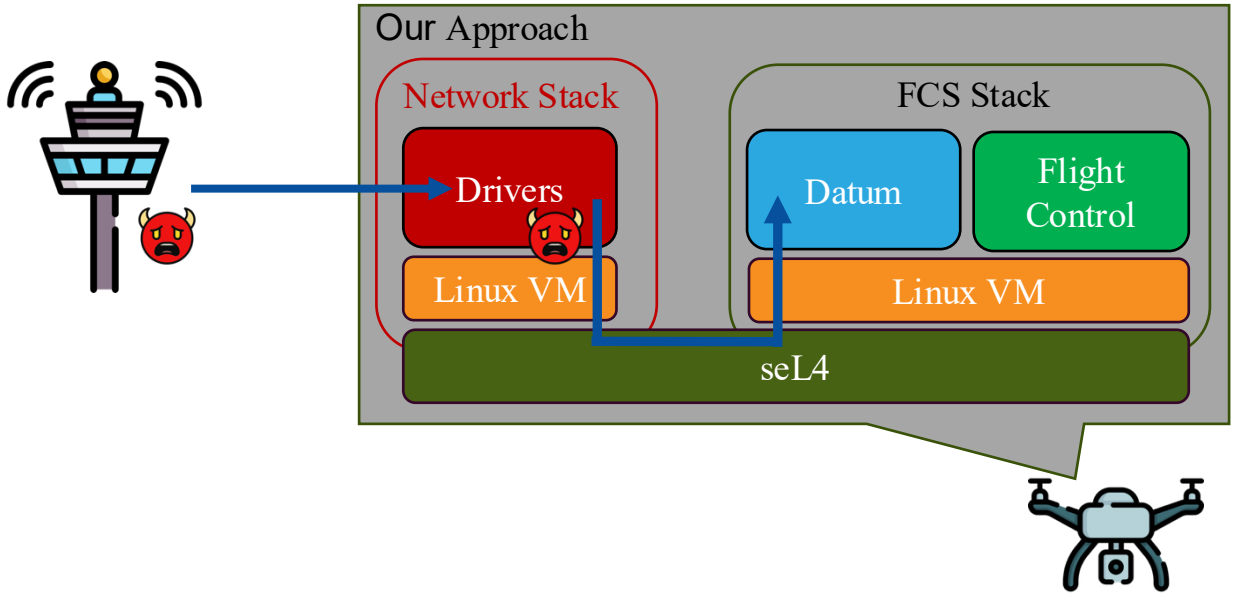


We show how to leverage runtime monitoring and high-assurance operating systems to defend against sophisticated adversaries.

Arthur Amorim
Arthur.Amorim@ucf.edu
https://art-amorim.github.io/

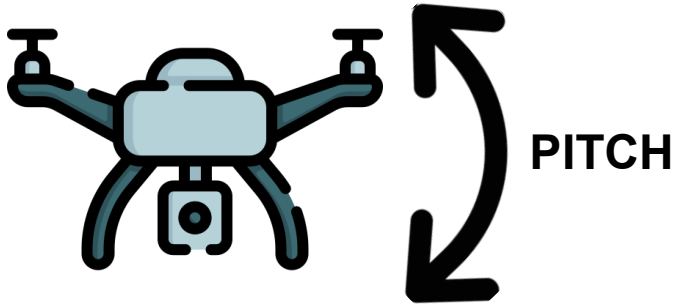
Dr. Max Taylor
maxhtaylor@proton.me
https://maxtaylor.dev





Case studies

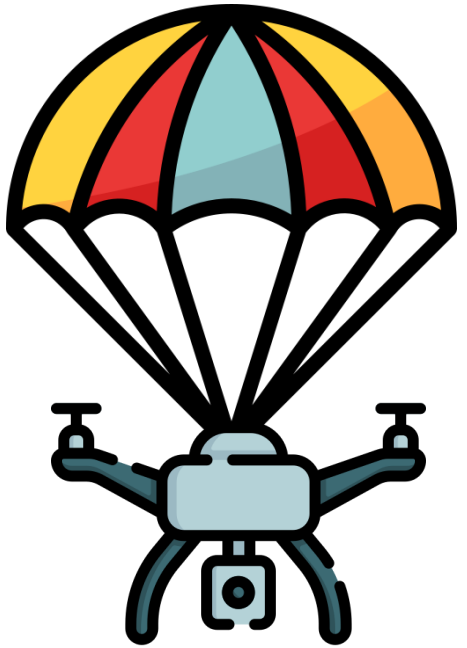
1- Inaccurate Bounds



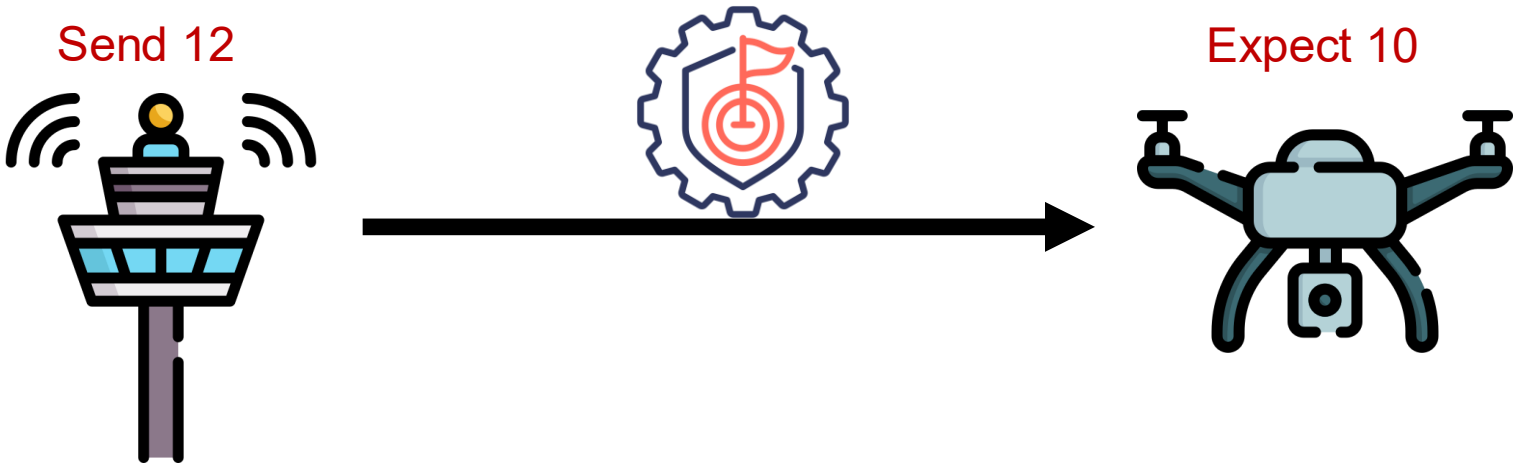
Pitch parameters

Parameter	Description
MC PITCH P	Pitch proportional gain
MC PITCHRATE P	Pitch rate proportional gain
MC PITCHRATE FF	Pitch rate feedforward
MC PITCHRATE MAX	Max pitch rate limit

2- Precondition Violation



3- Resource Misusage



Preconditions

1. The motors are armed.
2. flight mode not in FLIP or ACRO.
3. UAV is not gaining altitude.
4. altitude is above the CHUTE_ALT_MIN.

An attacker can exploit a vulnerability in the Linux wireless stack to compromise the Linux network drivers

CVE-2022-42719 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

A use-after-free in the mac80211 stack when parsing a multi-BSSID element in the Linux kernel 5.2 through 5.19.x before 5.19.16 could be used by attackers (able to inject WLAN frames) to crash the kernel and potentially execute code.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NVD **NIST:** NVD **Base Score:** 8.8 HIGH

Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2022-41674 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

An issue was discovered in the Linux kernel before 5.19.16. Attackers able to inject WLAN frames could cause a buffer overflow in the ieee80211_bss_info_update function in net/mac80211/scan.c.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NVD **NIST:** NVD **Base Score:** 8.1 HIGH

Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVE-2022-42720 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Various refcounting bugs in the multi-BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to trigger use-after-free conditions to potentially execute code.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

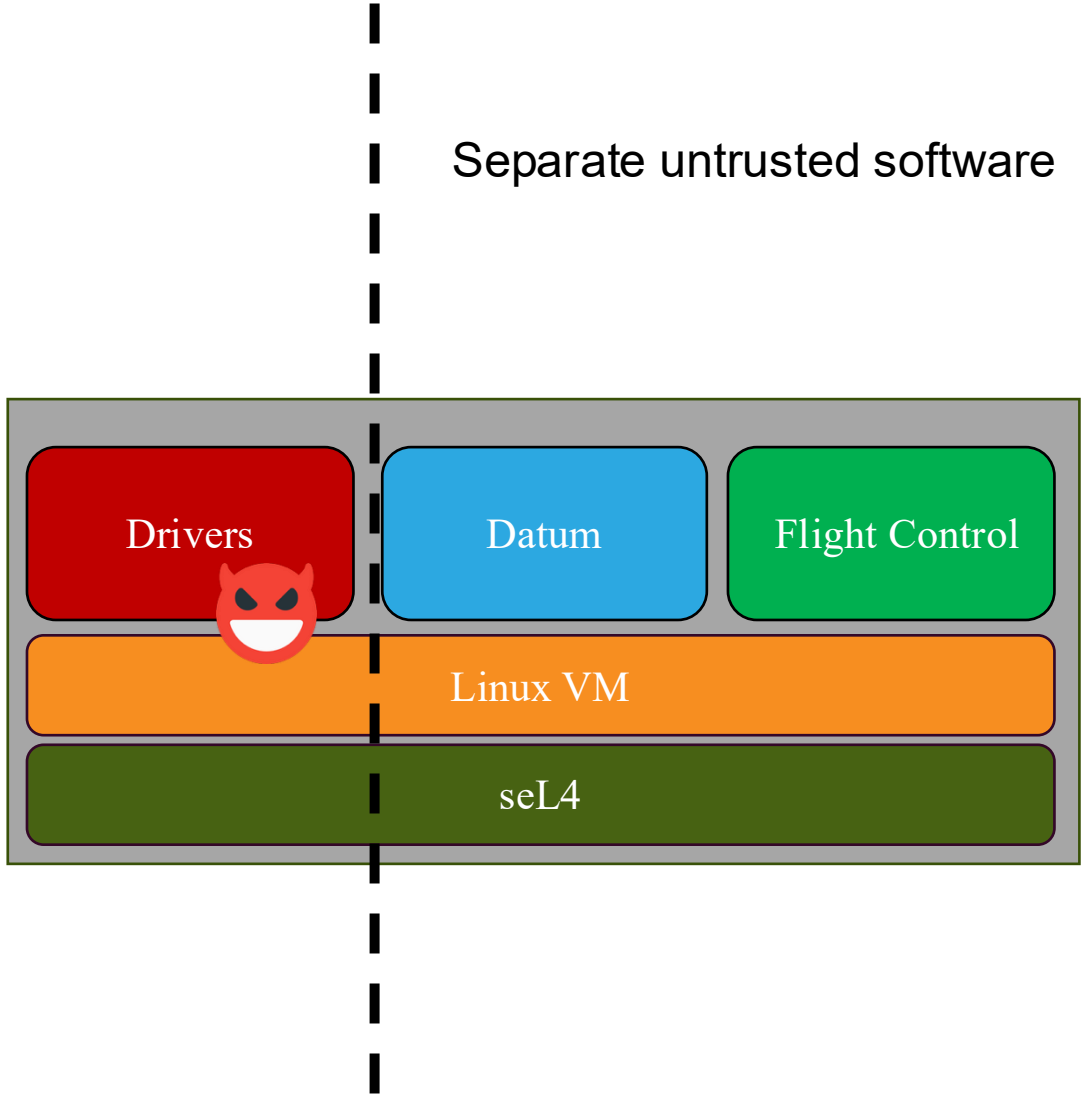
NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

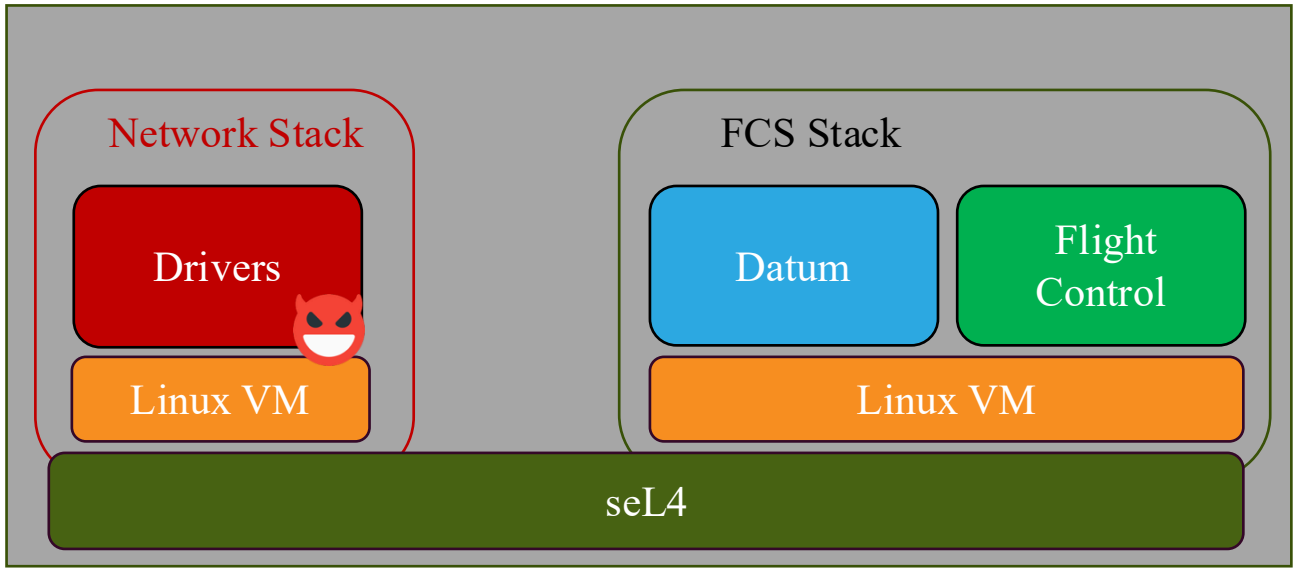
NVD **NIST:** NVD **Base Score:** 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

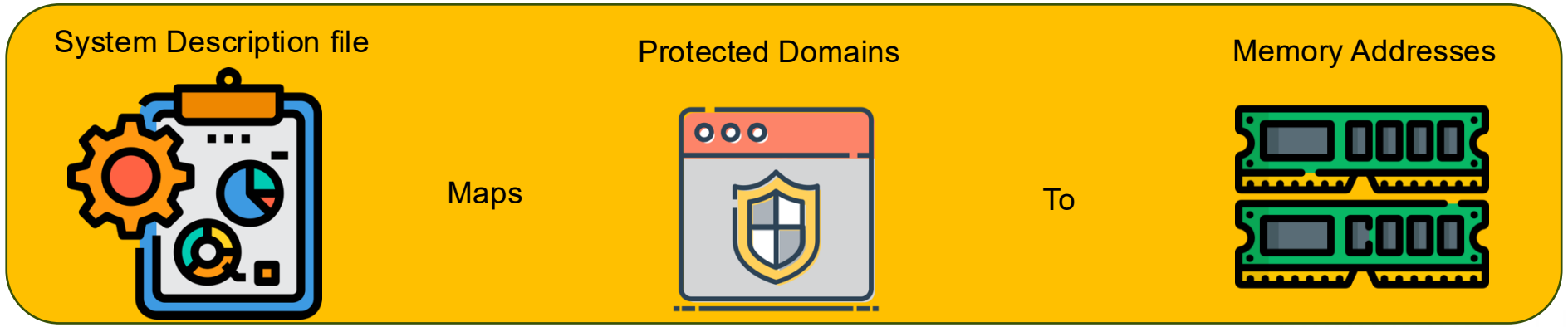
Challenge 1: Isolating the network stack from Datum and FCS



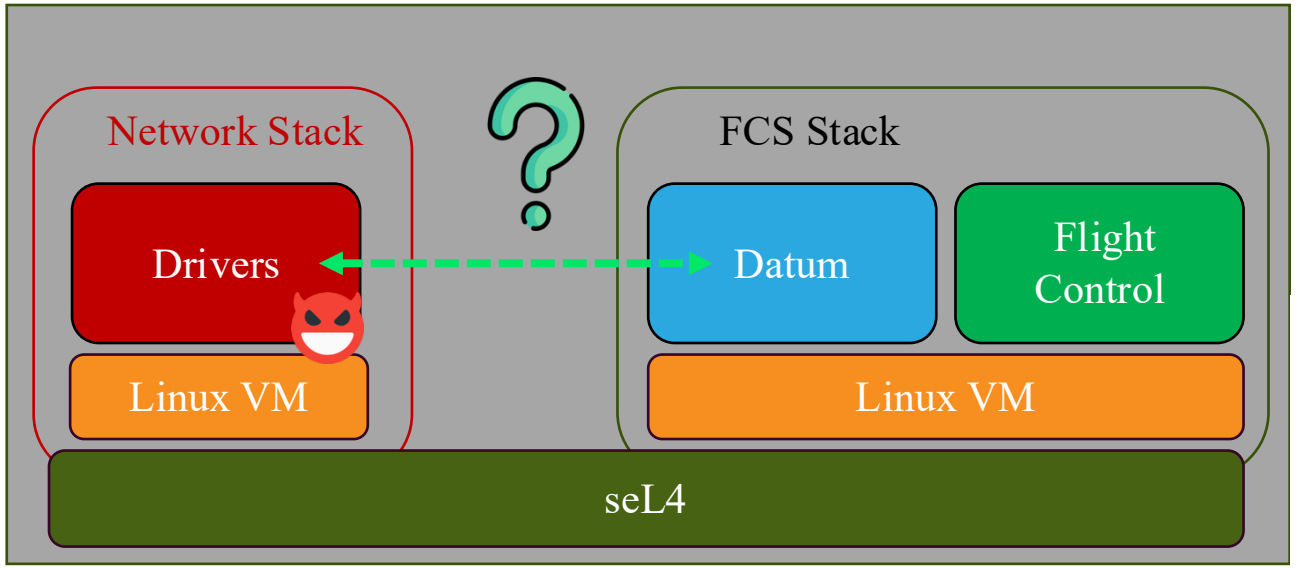
Challenge 1: Isolating the network stack from Datum and FCS



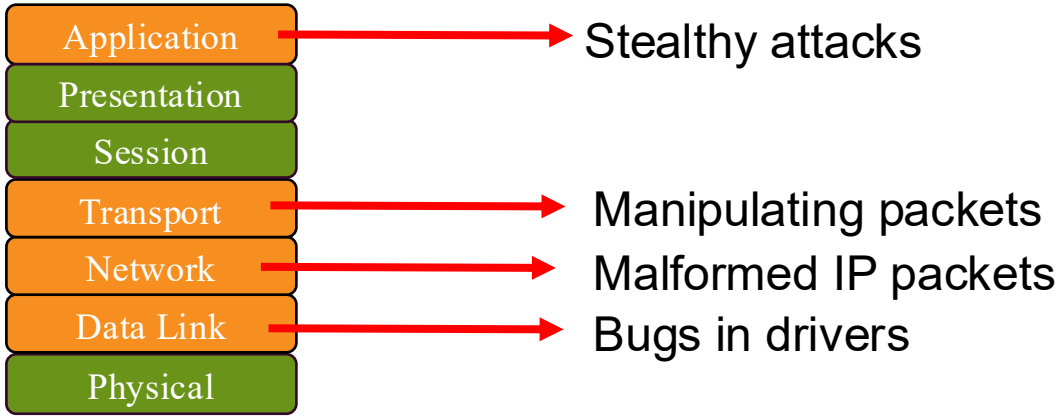
Approach : Memory regions not mapped into a protection domain are inaccessible to it.



Challenge 2: Enabling Safe Communications Between Components



TCP/IP Layers



CVE-1999-0804 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

Denial of service in Linux 2.2.x kernels via malformed ICMP packets containing unusual types, codes, and IP header lengths.

CVE-2016-7039 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.

CVE-2007-4567 Detail

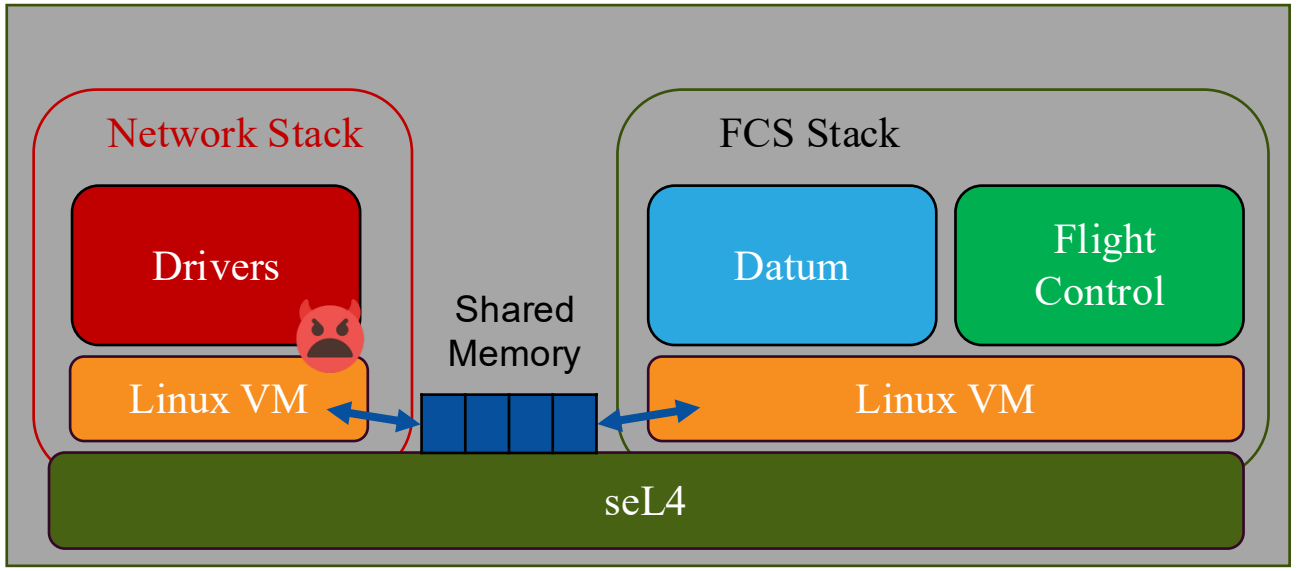
DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Current Description

The ipv6_hop_jumbo function in net/ipv6/exthdrs.c in the Linux kernel before 2.6.22 does not properly validate the hop-by-hop IPv6 extended header, which allows remote attackers to cause a denial of service (NULL pointer dereference and kernel panic) via a crafted IPv6 packet.

Challenge 2: Enabling Safe Communications Between Components



Approach : Messages are written and read from a shared memory buffer.

TCP/IP Layers

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

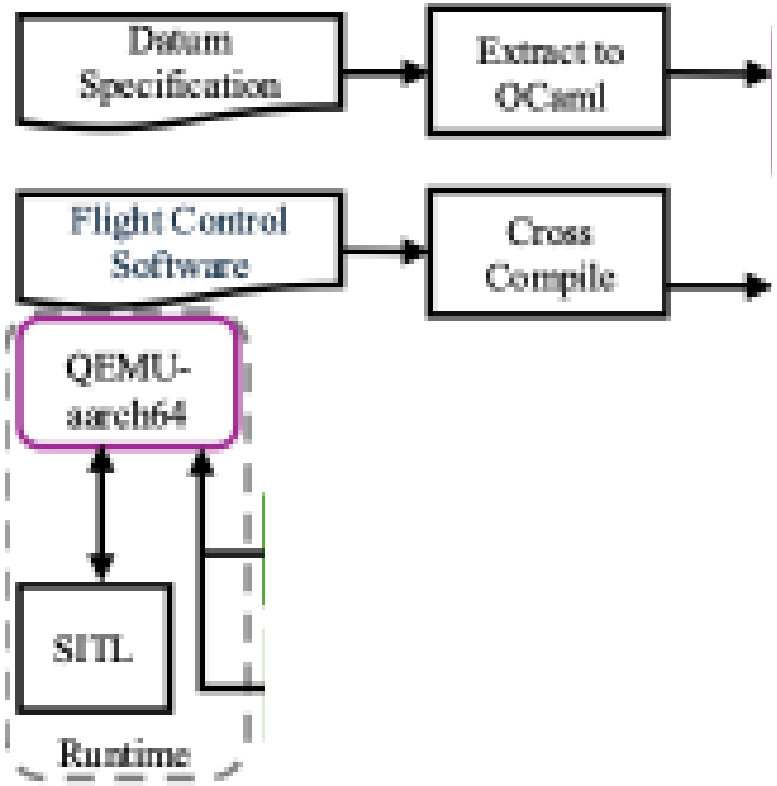
Stealthy attacks → Datum

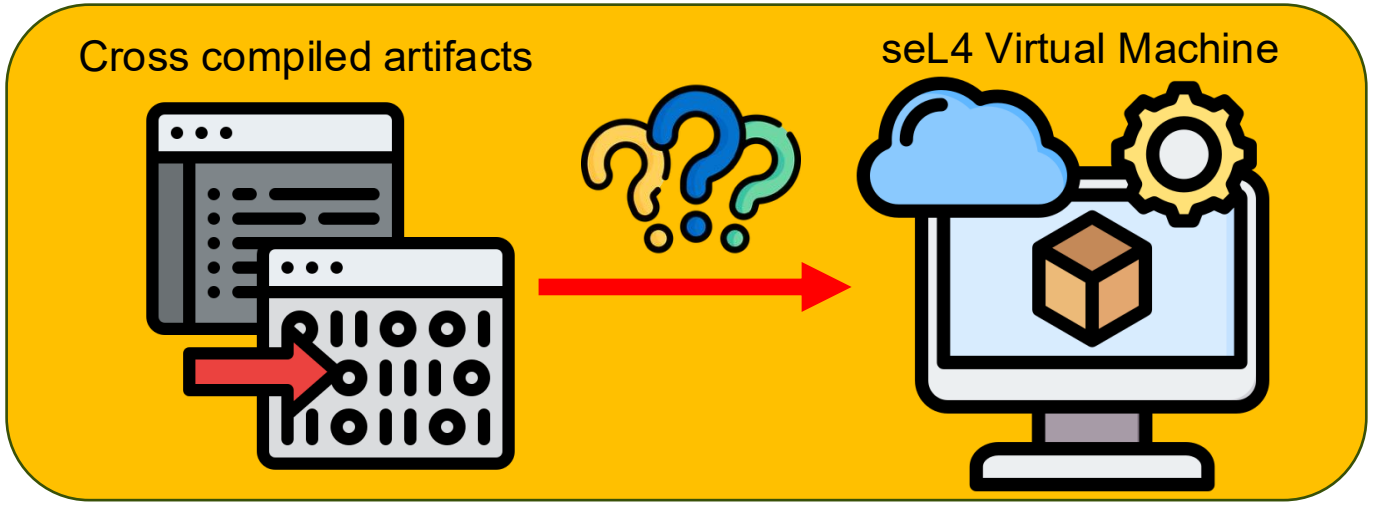
Manipulating packets → Predefined format

Malformed IP packets → Predefined format

Bugs in drivers → Virtual network devices

Challenge 3: Integrating the system





Challenge 3: Integrating the system