ART
ADVANCED SOLUTION

Driving Forward:
Security by Design in Automotive Industry

Security by Design [1/2]

Definition

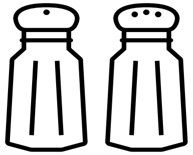
Security:

The state in which the integrity, confidentiality, and accessibility of information, service or network entity is assured [NISTIR 4734]

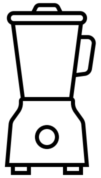
Security by Design [2/2]

Definition

What should we grasp?



✗



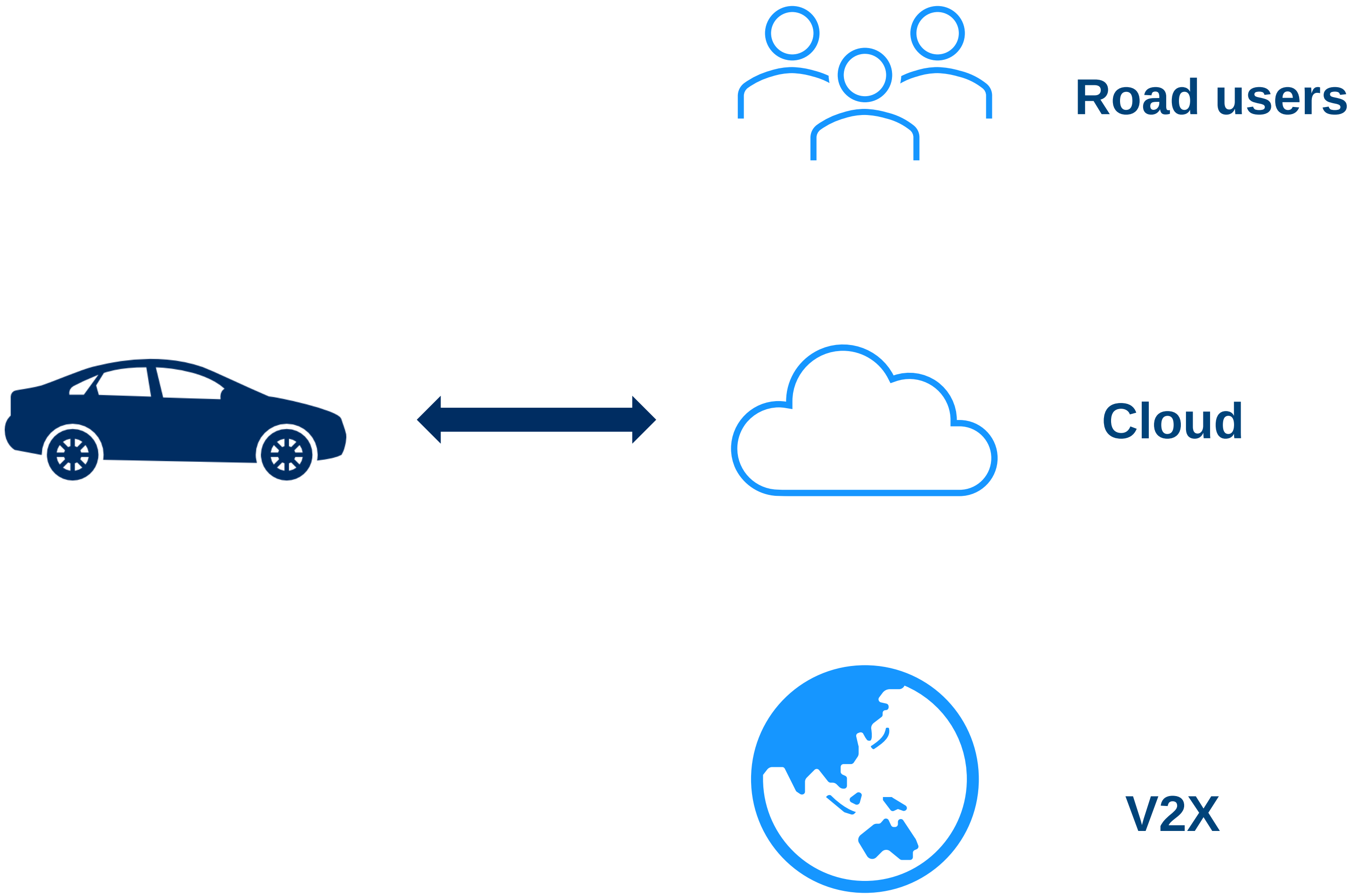
✓

Security by design expects to consider cybersecurity as a requirement so that the system can securely deliver intended functionalities.

Why Automotive needs Security by Design?

How Automotive has been evolving

CAN relies on *Security by Obscurity*



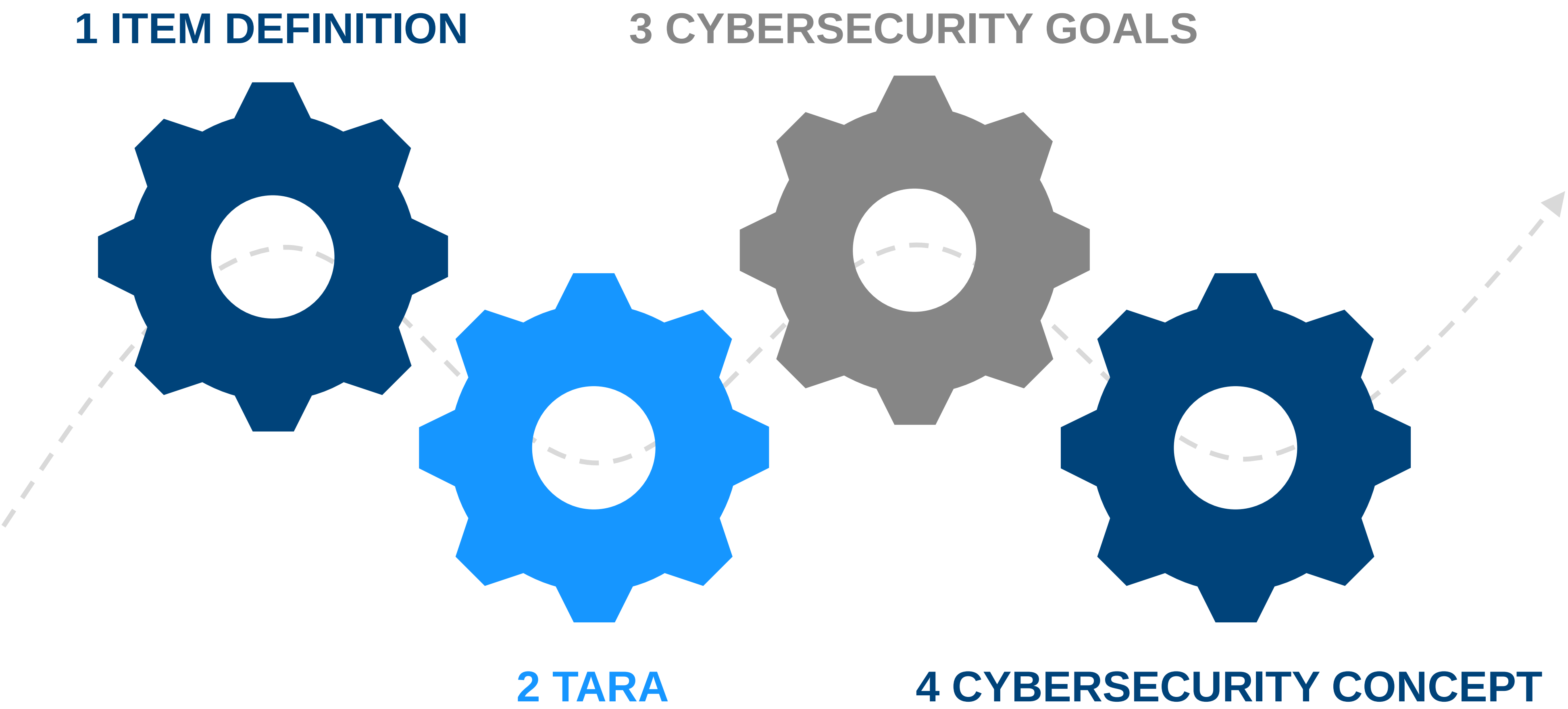
Road users

Cloud

V2X

How Automotive integrates Security By Design

ISO21434: The Concept Phase



1 ITEM DEFINITION

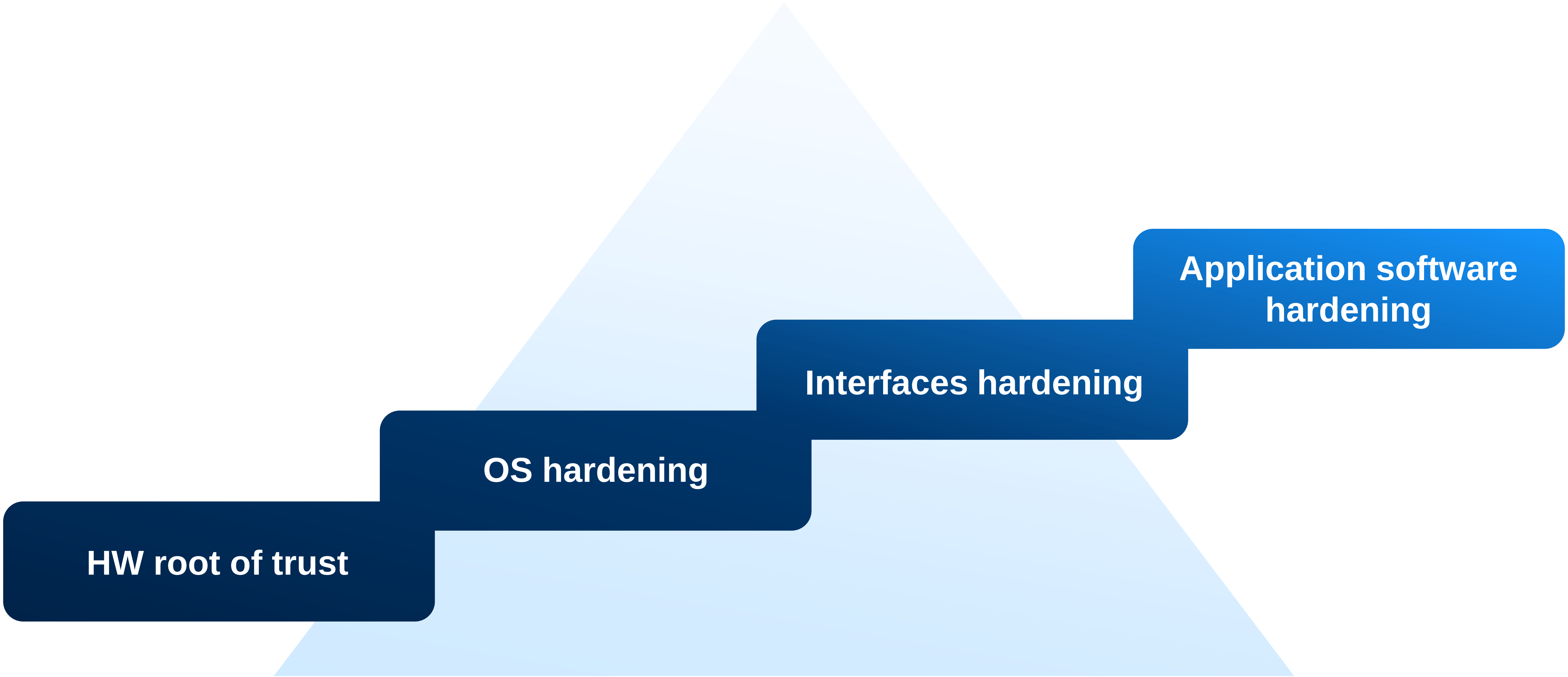
2 TARA

3 CYBERSECURITY GOALS

4 CYBERSECURITY CONCEPT

How Automotive implements Security By Design

Bottom-up strategy



HW root of trust

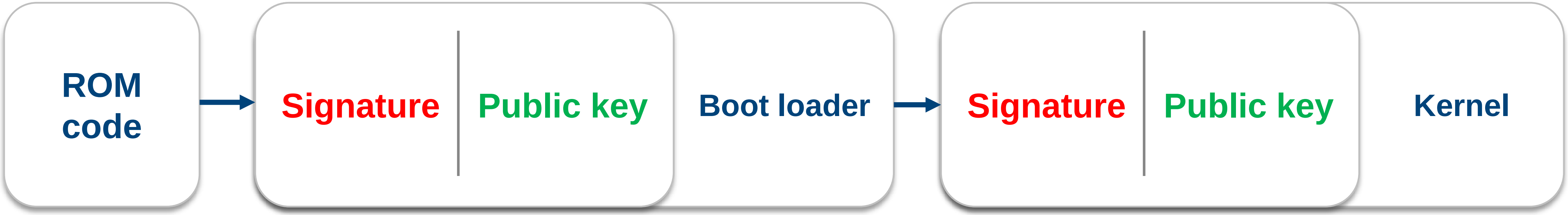
OS hardening

Interfaces hardening

Application software hardening

HW root of trust

Make sure to know your guests ☺



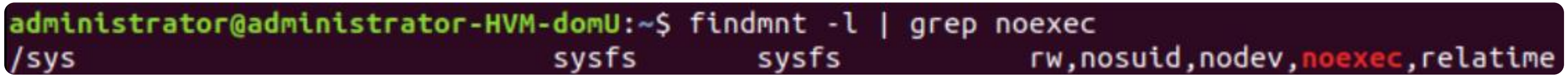
⚓ HASH (Public key)

HSM

OS hardening [1/2]

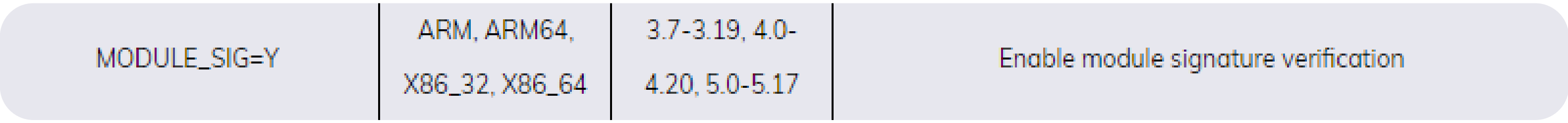
Do not let party at home ☺

Mounting



```
administrator@administrator-HVM-domU:~$ findmnt -l | grep noexec
/sys                           sysfs        sysfs              rw,nosuid,nodev,noexec,relatime
```

Harden your kernel



MODULE_SIG=Y	ARM, ARM64, X86_32, X86_64	3.7-3.19, 4.0-4.20, 5.0-5.17	Enable module signature verification

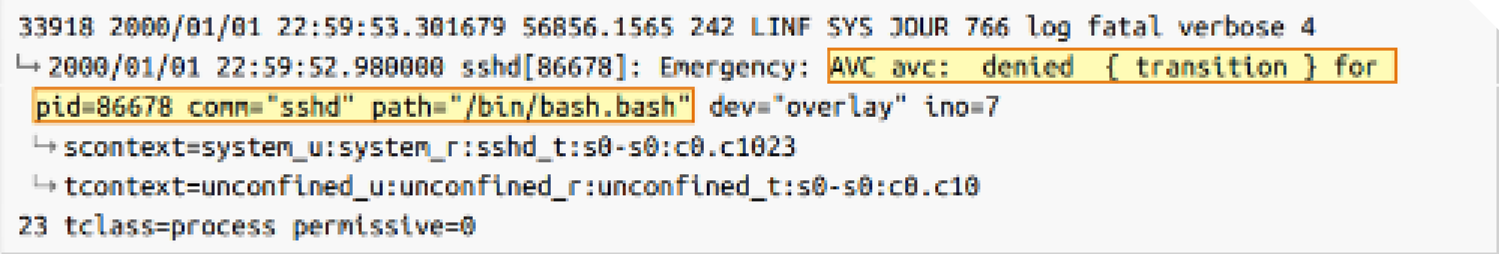
TimeSys

Avoid using legacy kernel versions

OS hardening [2/2]

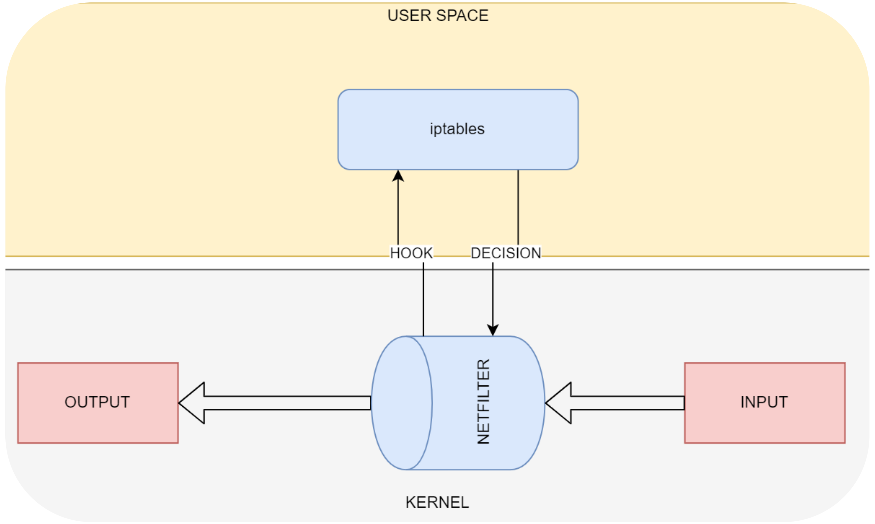
Do not let party at home ☺

Mandatory Access Control (SELINUX)



```
33918 2000/01/01 22:59:53.301679 56856.1565 242 LINF SYS JOUR 766 log fatal verbose 4
↳2000/01/01 22:59:52.980000 sshd[86678]: Emergency: AVC avc:  denied  { transition } for
 pid=86678 comm="sshd" path="/bin/bash.bash" dev="overlay" ino=7
 ↳scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023
 ↳tcontext=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c10
23 tclass=process permissive=0
```

Host-based firewall (iptables)

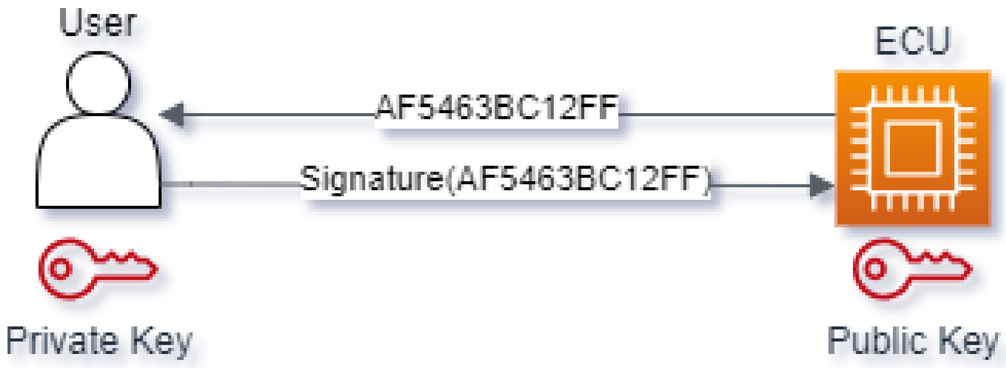


Interface hardening

Do not leave your door open ☺

Whitelist your USB ports

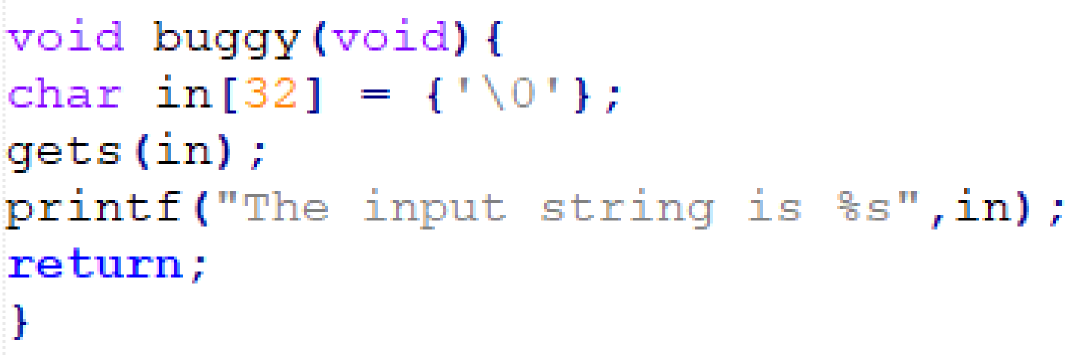
Authenticate your debug ports



Application software hardening

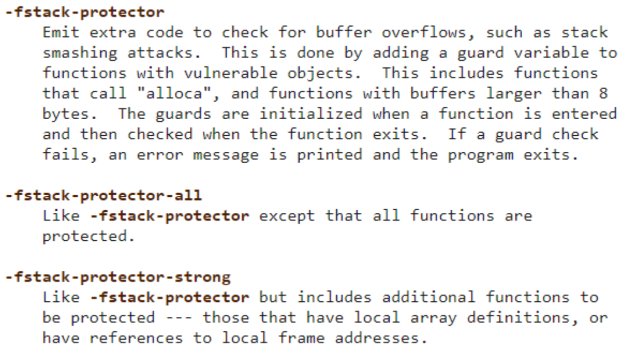
You know when your guests act up ☺

C/C++



```
void buggy(void){
char in[32] = {'\0'};
gets(in);
printf("The input string is %s",in);
return;
}
```

Mitigations

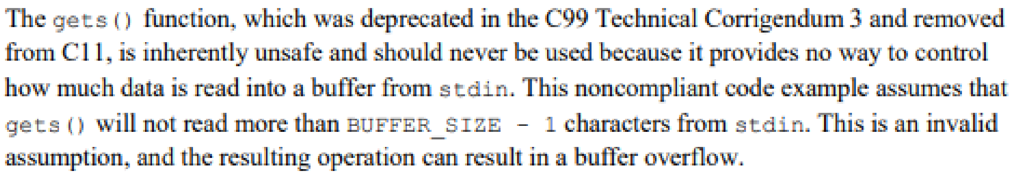


```
-fstack-protector
    Emit extra code to check for buffer overflows, such as stack
    smashing attacks.  This is done by adding a guard variable to
    functions with vulnerable objects.  This includes functions
    that call "alloca", and functions with buffers larger than 8
    bytes.  The guards are initialized when a function is entered
    and then checked when the function exits.  If a guard check
    fails, an error message is printed and the program exits.

-fstack-protector-all
    Like -fstack-protector except that all functions are
    protected.

-fstack-protector-strong
    Like -fstack-protector but includes additional functions to
    be protected --- those that have local array definitions, or
    have references to local frame addresses.
```

[gcc man page]



The `gets()` function, which was deprecated in the C99 Technical Corrigendum 3 and removed from C11, is inherently unsafe and should never be used because it provides no way to control how much data is read into a buffer from `stdin`. This noncompliant code example assumes that `gets()` will not read more than `BUFFER_SIZE - 1` characters from `stdin`. This is an invalid assumption, and the resulting operation can result in a buffer overflow.

[CERT C]

Minimize attack surface (AKA) Software BOM minimization

Wrap up

- Security by design **can** be applied to Automotive systems.
- Security by design **shall** be applied to Automotive systems.
- Resources and awareness have been rising e.g., MITRE embedded EMB3D for RISK assessment.
- Practice makes perfect.

Question time

See you next time ☺

ART
ADVANCED SOLUTION

www.artgroup-spa.com

BERLIN
TURIN
MODENA
TORRITA DI SIENA
PASSIGNANO

ART GERMANY

MATE ADVANCED LABORATORY