list cea tech

THALES

Formal code security

Challenge: code vulnerabilities

The FormalLab team was tasked to examine the use of code analysis tools for cybersecurity purposes.

We confronted security components and their requirements to the Frama-C source code analysis platform.

frama C Software Analyzers

Innovation: mathematical guarantees

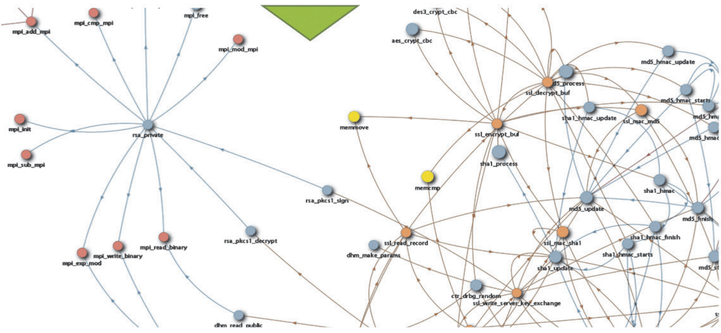
Plain requirements are lifted into precise, unambiguous formal specifications. The launch of dedicated analyzers provides mathematical guarantees that the software matches its specifications.

E 1.2.1 Function input parameters are valid.
E 4.1 Heap and stack integrity is guaranteed during the execution of each function.
E 5.1. A function operating on sensitive data shall not provide access to this data.

```
//@ requires 0 <= md->curlen < sizeof(md->buf);
error_t SHA256_update(SHA256_ctx_t *md, const uint8_t *data, …);

 //@ assert mem_access: \valid(x[i+1]);
 x[i+1] |= x[i] >> 31;

//@ assigns *Qx \from pECDHInstance, *pECDHInstance, d, *d,
d_Bytelength;
error_t ECDH_keyDerivation_ByteArray(ECC_Domain_t *pECDHInstance,
 uint8_t *d, unsigned long d_Bytelength, uint8_t *Qx, uint8_t *Qy);
```



Perpectives

Thales develops further pilots to validate operational usages of formal methods in development processes.

The FormalLab team assists Thales in this mission, and prepares to tackle the next generation of challenges in software and systems verification.

Contact

florent.kirchner@cea.fr
jean-marc.mota@thalesgroup.com

INSTITUT CARNOT TN@UPSaclay

université PARIS-SACLAY

Stand 26