

Journey to a RTE-free X.509 parser (with Frama-C)



{LRP, LSL, LSC}

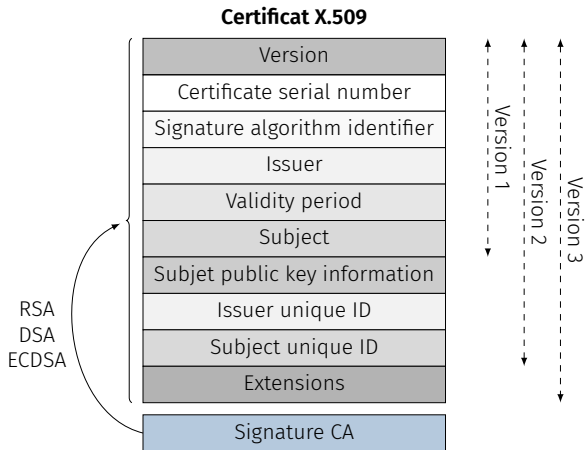
ANSSI

prenom.nom@ssi.gouv.fr

6 juin 2019

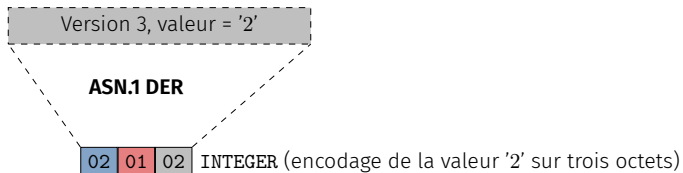
X.509 : BIENVENUE EN ENFER

- X.509 : format d'encodage des certificats



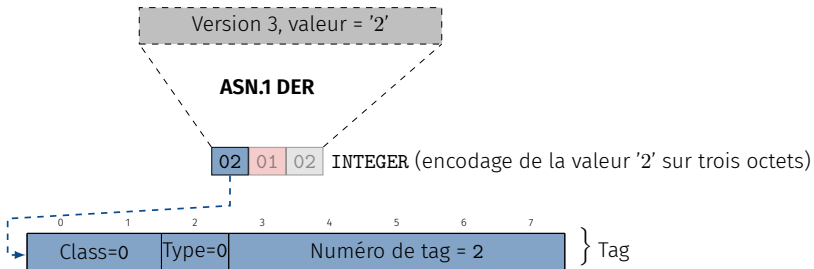
X.509 : BIENVENUE EN ENFER

- X.509 : format d'encodage des certificats
- Se base sur l'ASN.1 pour l'encodage et le décodage



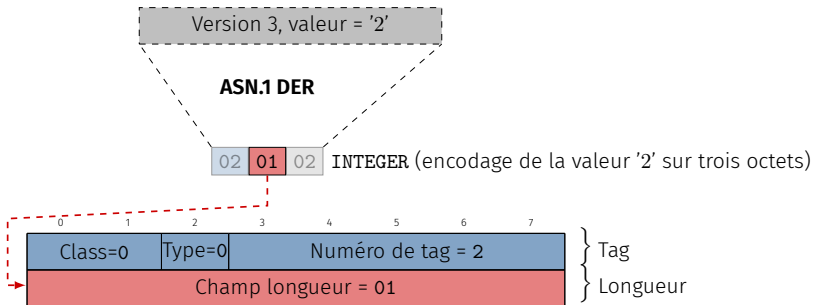
X.509 : BIENVENUE EN ENFER

- X.509 : format d'encodage des [certificats](#)
- Se base sur l'[ASN.1](#) pour l'encodage et le décodage



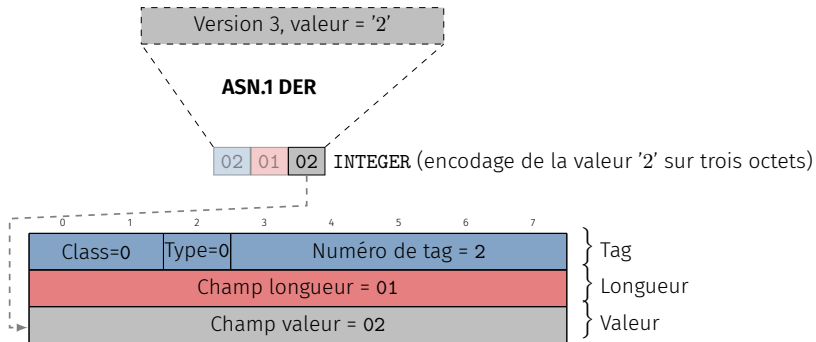
X.509 : BIENVENUE EN ENFER

- X.509 : format d'encodage des [certificats](#)
- Se base sur l'[ASN.1](#) pour l'encodage et le décodage



X.509 : BIENVENUE EN ENFER

- X.509 : format d'encodage des certificats
- Se base sur l'ASN.1 pour l'encodage et le décodage



\$ dumpasn1 cert.der (1.6 KB)

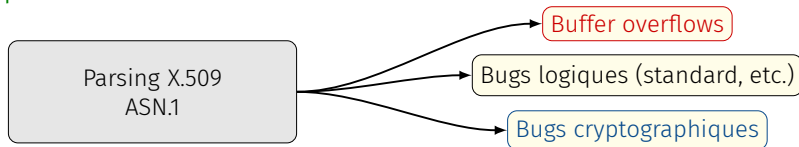
```

0 1665: SEQUENCE {
4 1385: SEQUENCE {
8 3: [0] {
10 1: INTEGER 2
13 8: INTEGER 68 53 A2 BA 39 45 04 A0
23 13: SEQUENCE {
25 9: OBJECT IDENTIFIER sha1WithRSAEncryption (1 2 840
113549 1 1 5)
36 0: NULL
38 73: SEQUENCE {
40 11: SET {
42 9: SEQUENCE {
44 3: OBJECT IDENTIFIER countryName (2 5 4 6)
49 2: PrintableString 'US'
53 19: SET {
55 17: SEQUENCE {
57 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
62 10: PrintableString 'Google Inc'
74 37: SET {
76 35: SEQUENCE {
78 3: OBJECT IDENTIFIER commonName (2 5 4 3)
83 28: PrintableString 'Google Internet Authority G2'
113 30: SEQUENCE {
115 13: UTCTime 09/04/2014 11:21:21 GMT
130 13: UTCTime 08/07/2014 00:00:00 GMT
145 102: SEQUENCE {
147 11: SET {
149 9: SEQUENCE {
151 3: OBJECT IDENTIFIER countryName (2 5 4 6)
156 2: PrintableString 'US'
160 19: SET {
162 17: SEQUENCE {
164 3: OBJECT IDENTIFIER stateOrProvinceName (2 5 4
8)
169 10: UTF8String 'California'
181 22: SET {
183 20: SEQUENCE {
185 3: OBJECT IDENTIFIER localityName (2 5 4 7)
190 13: UTF8String 'Mountain View'
205 19: SET {
207 17: SEQUENCE {
209 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
214 10: UTF8String 'Google Inc'
226 21: SET {
228 19: SEQUENCE {
230 3: OBJECT IDENTIFIER commonName (2 5 4 3)
235 12: UTF8String '*.google.com'
249 89: SEQUENCE {
251 19: SEQUENCE {
253 7: OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2
1)
262 8: OBJECT IDENTIFIER prime256v1 (1 2 840 10045 3 1
7)
272 66: BIT STRING
04 5D 5F 79 E6 D8 17 61 2C 9E 3D 24 BC 88 98 24
1F C7 AC AS 38 DE 82 D8 95 94 90 A4 58 53 08 CB
26 99 E0 FA 52 B8 3C 4A 50 F3 46 30 BE D0 0F D2
81 52 D0 2F D3 DC 9A 2F 88 A1 2C C3 2B 1B E8 AF
5F
[3] SEQUENCE {
340 1049: OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
344 1045: OCTET STRING, encapsulates {
348 29: SEQUENCE {
350 3: OBJECT IDENTIFIER serverAuth (1 3 6 1 5 5
7 3 1)
355 22: OCTET STRING, encapsulates {
357 20: OBJECT IDENTIFIER clientAuth (1 3 6 1 5 5
7 3 2)
359 8: SEQUENCE {
379 738: OBJECT IDENTIFIER subjectAltName (2 5 29 17)
383 3: OCTET STRING, encapsulates {
388 729: SEQUENCE {
392 725: [2] *.google.com'
396 12: [2] *.android.com'
410 13: [2] *.appengine.google.com'
425 22: [2] *.cloud.google.com'
449 18: [2] *.google-analytics.com'
469 22: [2] *.google.ca'
493 11: [2] *.google.cl'
506 11: [2] *.google.co.in'
519 14: [2] *.google.co.jp'
535 14: [2] *.google.co.uk'
551 14: [2] *.google.com.ar'
567 15: [2] *.google.com.au'
584 15: [2] *.google.com.br'
597 15: [2] *.google.com.mx'
618 15: [2] *.google.com.sa'
635 15: [2] *.google.com.tr'
652 15: [2] *.google.com.vn'
669 15: [2] *.google.de'
686 11: [2] *.google.es'
699 11: [2] *.google.fr'
712 11: [2] *.google.hu'
725 11: [2] *.google.it'
738 11: [2] *.google.nl'
751 11: [2] *.google.pl'
764 11: [2] *.google.pt'
777 11: [2] *.googleapic.cn'
790 15: [2] *.googlecommerce.com'
807 20: [2] *.googlevideo.com'
829 17: [2] *.gstatic.com'
848 13: [2] *.gvt1.com'
863 10: [2] *.urchin.com'
875 12: [2] *.urchin.com'
889 16: [2] *.url.google.com'
907 22: [2] *.youtube-nocookie.com'
931 13: [2] *.youtube.com'
946 22: [2] *.youtubeeducation.com'
970 11: [2] *.ytimg.com'
983 11: [2] *.android.com'
996 4: [2] g.co'
1002 6: [2] geo.gl'
1010 20: [2] *.google-analytics.com'
1032 10: [2] *.google.com'
1044 18: [2] *.googlecommerce.com'
1064 10: [2] *.urchin.com'
1076 8: [2] *.youtu.be'
1086 11: [2] *.youtube.com'
1099 20: [2] *.youtubeeducation.com'
1121 11: SEQUENCE {
1123 3: OBJECT IDENTIFIER keyUsage (2 5 29 15)
1128 4: OCTET STRING, encapsulates {
1130 2: BIT STRING 7 unused bits
1132 2: '1'B (bit 0)
1134 104: SEQUENCE {
1136 8: OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1
5 5 7 1 1)
1148 92: OCTET STRING, encapsulates {
1148 90: SEQUENCE {
1150 43: SEQUENCE {
1152 8: OBJECT IDENTIFIER cAIssuers (1 3 6 1 5 5
7 48 2)
1162 31: [6] 'http://pki.google.com/GIAG2.crt'
1195 43: SEQUENCE {
1197 8: OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48
1)
1207 31: [6] 'http://clients1.google.com/ocsp'
1240 29: SEQUENCE {
1242 3: OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29
14)
1247 22: OCTET STRING, encapsulates {
1249 20: OCTET STRING
23 D8 36 C8 19 D5 01 C3 32 A9 77 01 69 ED
70 B3
97 AF 00 F4
1271 12: SEQUENCE {
1273 3: OBJECT IDENTIFIER basicConstraints (2 5 29 19)
1278 1: BOOLEAN TRUE
1281 2: OCTET STRING, encapsulates {
1283 0: SEQUENCE {}
1285 31: SEQUENCE {
1287 3: OBJECT IDENTIFIER authorityKeyIdentifier (2 5
29 35)
1292 24: OCTET STRING, encapsulates {
1294 22: SEQUENCE {
1296 20: [0]
4A DD 06 16 1B BC FB 68 B5 76 F5 81 B6
BB 62 1A
BA 5A 81 2F
1318 23: SEQUENCE {
1320 3: OBJECT IDENTIFIER certificatePolicies (2 5 29
32)
1325 16: OCTET STRING, encapsulates {
1327 14: SEQUENCE {
1329 12: SEQUENCE {
1331 10: OBJECT IDENTIFIER '1 3 6 1 4 1 1129 2 5
1'
1343 48: SEQUENCE {
1345 3: OBJECT IDENTIFIER cRLDistributionPoints (2 5
29 31)
1350 41: OCTET STRING, encapsulates {
1352 39: SEQUENCE {
1354 37: SEQUENCE {
1356 35: [0]
1358 33: [0]
1360 31: [6] 'http://pki.google.com/GIAG2.crl'
1393 13: SEQUENCE {
1395 9: OBJECT IDENTIFIER sha1WithRSAEncryption (1 2 840
113549 1 1 5)
1406 0: NULL
1408 257: BIT STRING
9A AB AC 28 75 DA 3A FB 64 54 7E DD 6B 6B B8 05
B8 08 43 36 91 DE 87 06 B1 C3 AF A2 03 B9 E8 87
FB 34 39 3B 6E C7 DE C3 79 96 83 96 AB AF 3F 34
F3 0F 1C 13 56 6C A5 04 B9 44 71 1F 60 2F C8 91
51 C7 B4 80 A9 E8 0D 28 89 BE 9C AC 71 6D 50 9E
88 1D 0F 87 52 D6 27 62 FF 98 D8 34 4D 07 FC DD
05 9B 64 91 2E 53 E3 9E 46 87 A5 FD 46 E7 4B 42
38 1D 48 32 7D 63 E6 DB EA F8 43 0C 80 C3 3B 5F
C8 33 05 93 D4 88 BD 81 51 73 8E 6A 20 3E D8 C6
91 9E 80 3B CA 1D 70 85 EB DD 79 FD 4E 76 A1 37
97 51 FE D0 AF B9 7C CF 87 AB 24 DE 27 8A ED 3F
06 69 AA 31 2D 4C F5 63 C7 B8 01 A5 4D 9D 37 C2
89 22 B3 0E 95 D9 A7 37 B3 F8 87 68 1A 9A 6E EB
7E 20 80 C6 EC FF 40 CE FB 48 29 18 08 04 C6 35
87 87 B6 F5 57 E0 FB F6 F2 5C D1 7D FA 5F 0D
5C 78 F6 24 EE C9 95 64 D3 A7 2A C5 F1 B6 1D

```

X.509/ASN.1 : YOUR CVE PROVIDER SINCE 1999

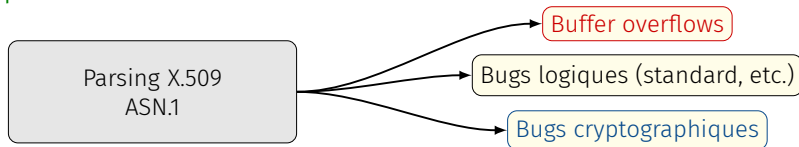
Complexité induit vulnérabilité



Paradoxal pour une brique censée amener de la sécurité !

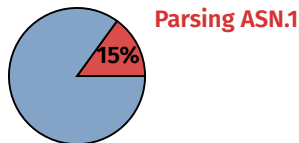
X.509/ASN.1 : YOUR CVE PROVIDER SINCE 1999

Complexité induit vulnérabilité



Paradoxal pour une brique censée amener de la sécurité !

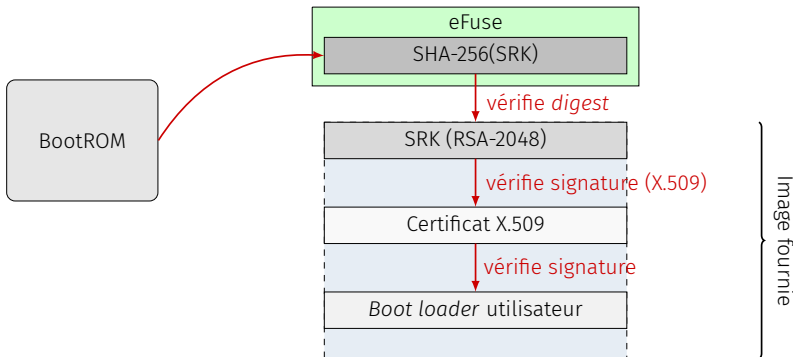
CVE OpenSSL depuis 1999 :



X.509/ASN.1 : YOUR CVE PROVIDER SINCE 1999

CVE-2017-7932

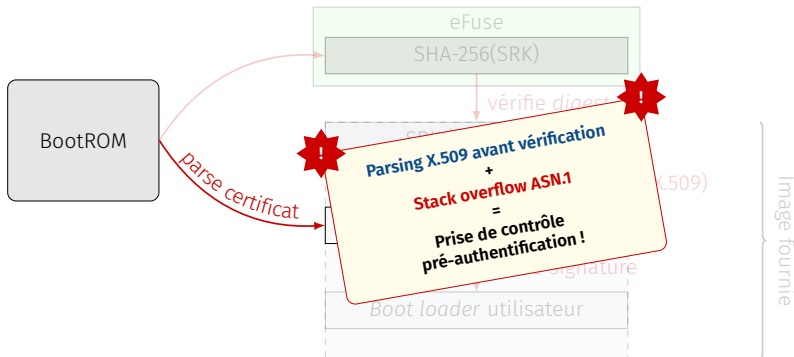
HAB (*High Assurance Boot*) des SoC i.MX28 à i.MX7 compromis (BootROM, irréversible)



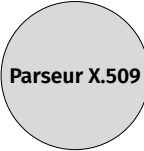
X.509/ASN.1 : YOUR CVE PROVIDER SINCE 1999

CVE-2017-7932

HAB (*High Assurance Boot*) des SoC i.MX28 à i.MX7 compromis (BootROM, irréversible)

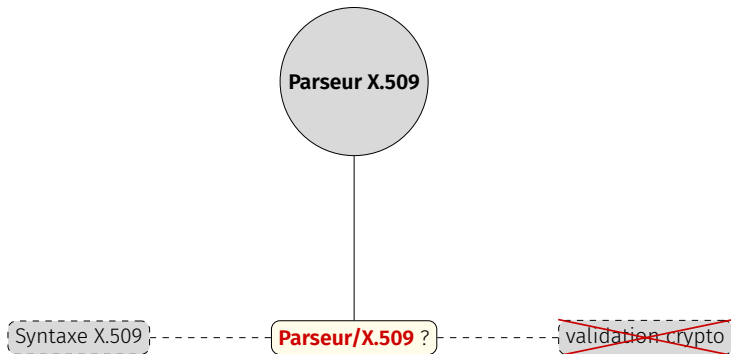


UN PARSEUR X.509 EN C "PROPRE" ?

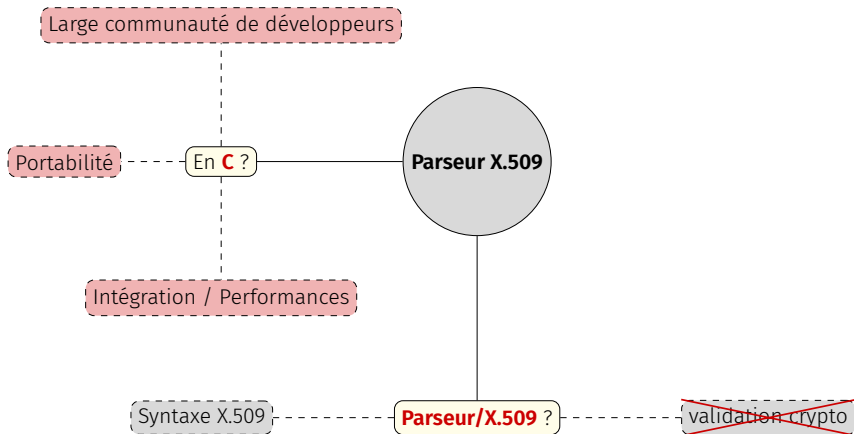


Parseur X.509

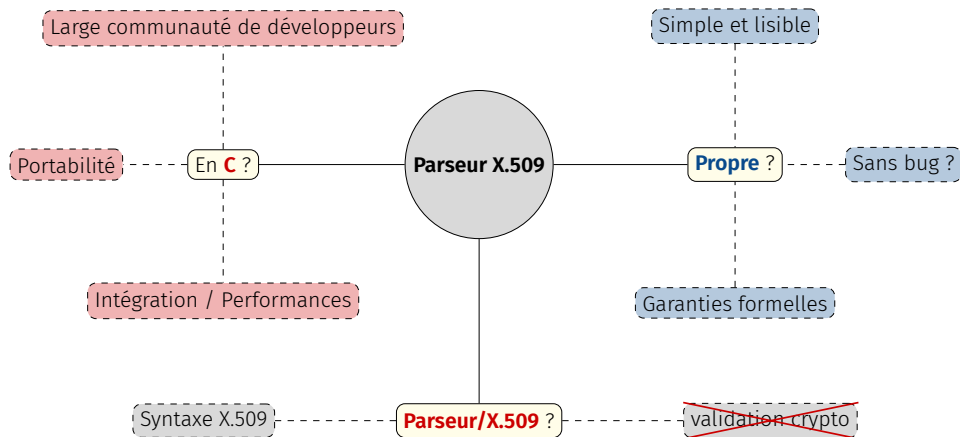
UN PARSEUR X.509 EN C "PROPRE" ?



UN PARSEUR X.509 EN C "PROPRE" ?

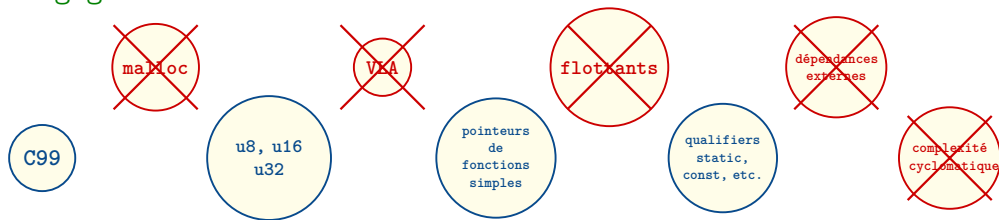


UN PARSEUR X.509 EN C "PROPRE" ?



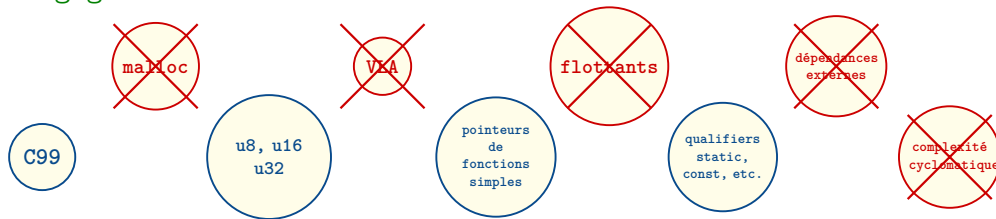
DÉVELOPPEMENT

Langage C



DÉVELOPPEMENT

Langage C

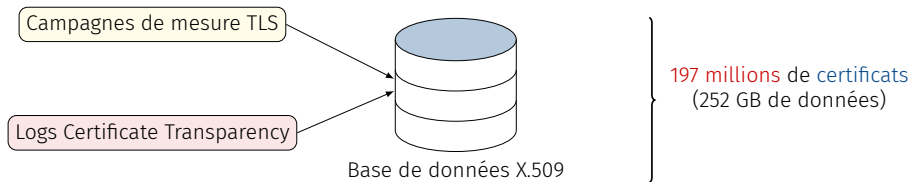


options de compilation strictes

```
clang -Weverything -Werror -pedantic -fno-builtin -D_FORTIFY_SOURCE=2 \
      -fstack-protector-strong -std=c99 -O3 -fPIC -ffreestanding \
      -Wno-reserved-id-macro -Wno-unreachable-code-break \
      -Wno-covered-switch-default -Wno-padded \
      -c x509_parser.c -o x509_parser.o
```

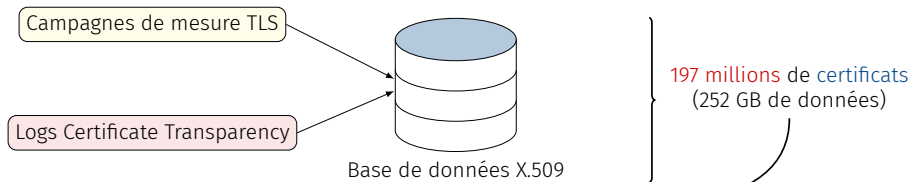
DATA SET

Origine et contenu



DATA SET

Origine et contenu

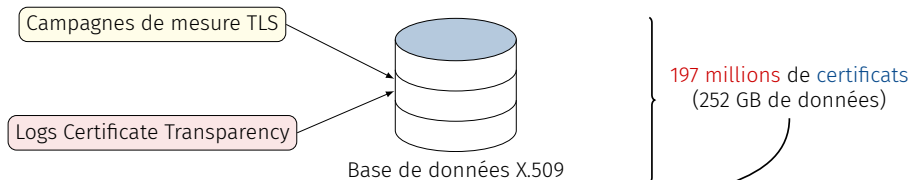


Intérêts

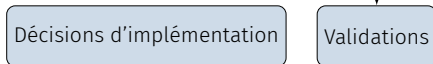
Décisions d'implémentation

DATA SET

Origine et contenu

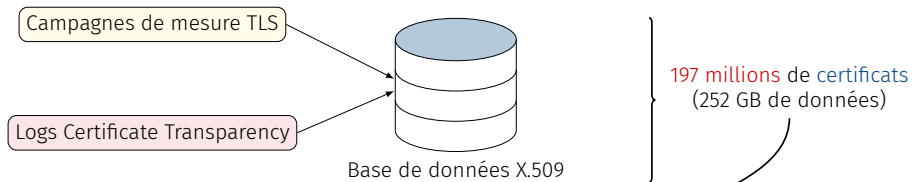


Intérêts



DATA SET

Origine et contenu

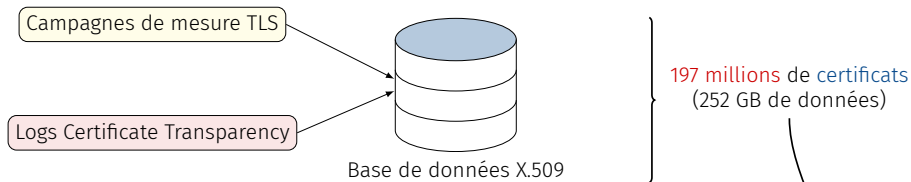


Intérêts



DATA SET

Origine et contenu



Intérêts

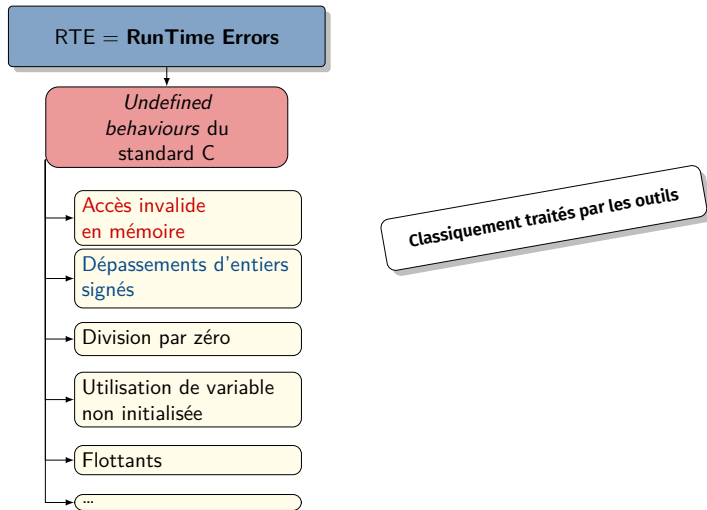
Décisions d'implémentation

Validations

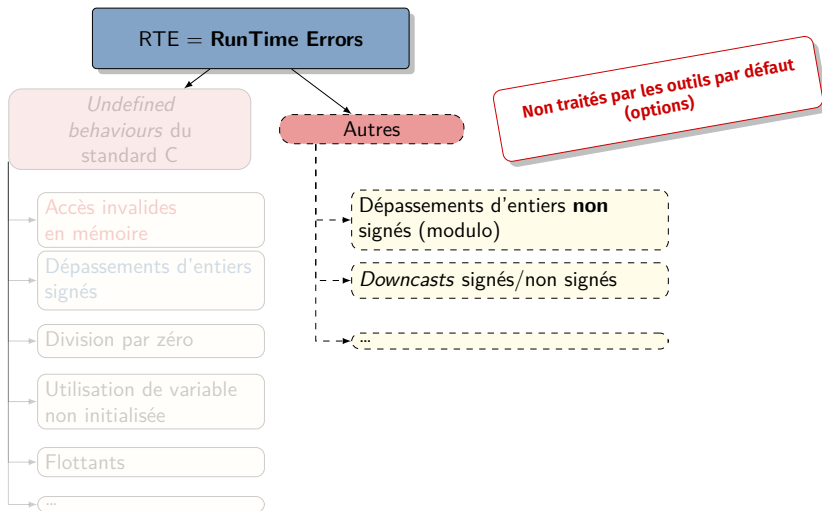
Non régression

Optimisation/performances
(200.000 certificats/seconde)

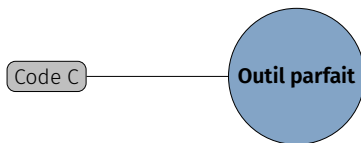
ABSENCE COMPLÈTE DE RTE ?



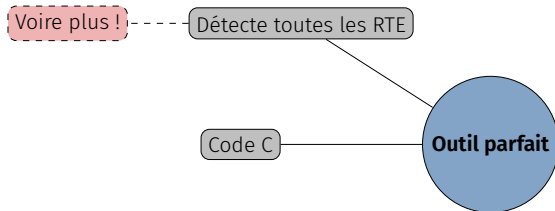
ABSENCE COMPLÈTE DE RTE ?



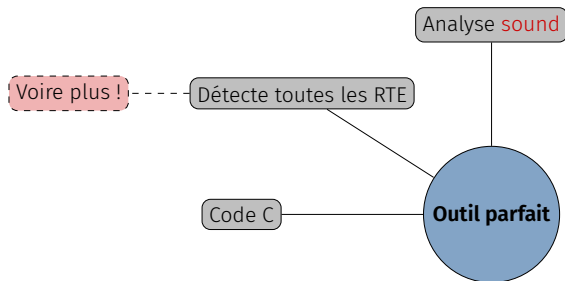
CHOIX DES ARMES



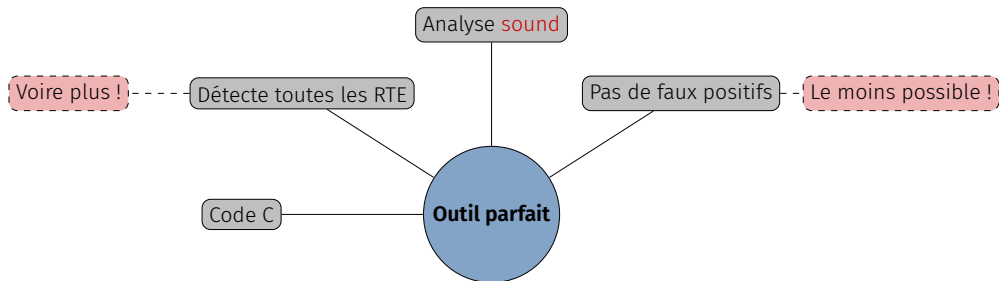
CHOIX DES ARMES



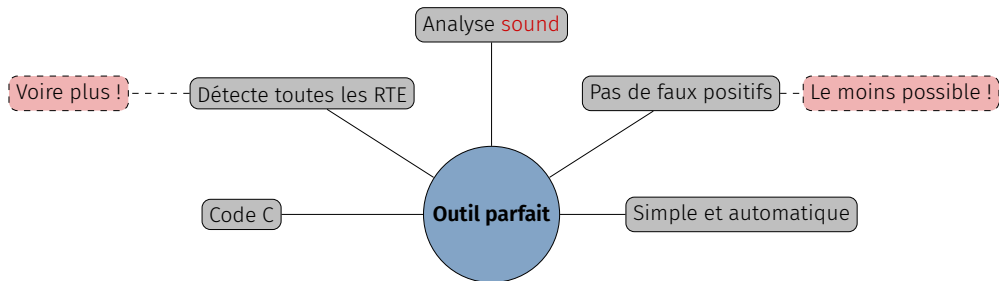
CHOIX DES ARMES



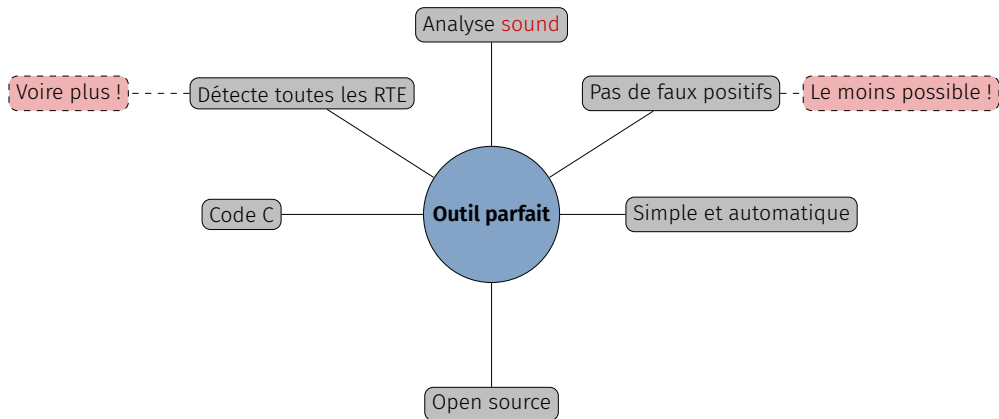
CHOIX DES ARMES



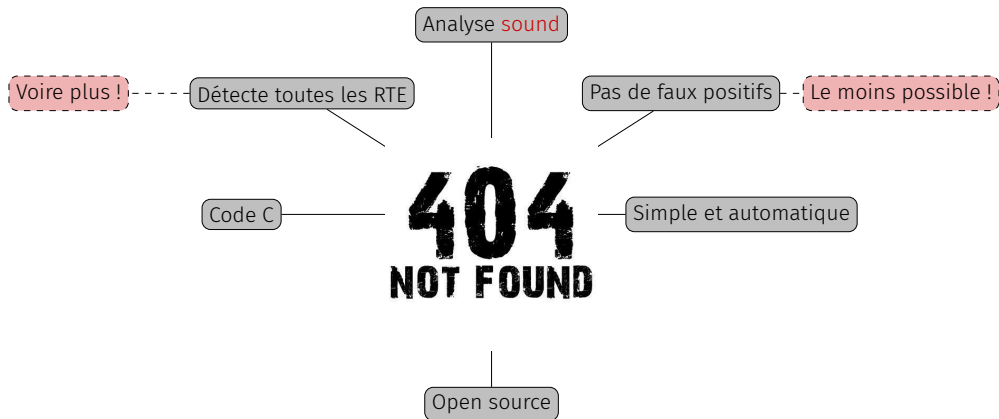
CHOIX DES ARMES



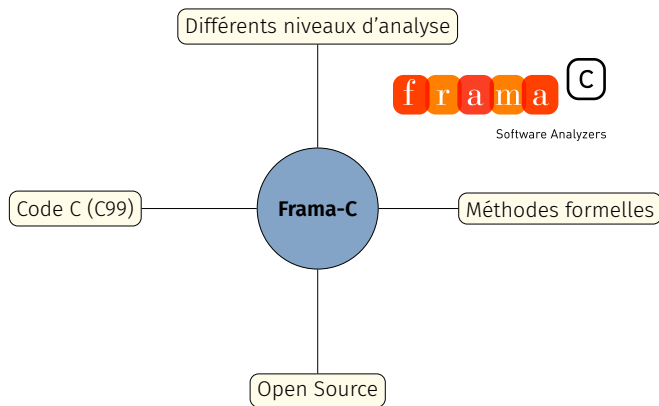
CHOIX DES ARMES



CHOIX DES ARMES



FRAMA-C

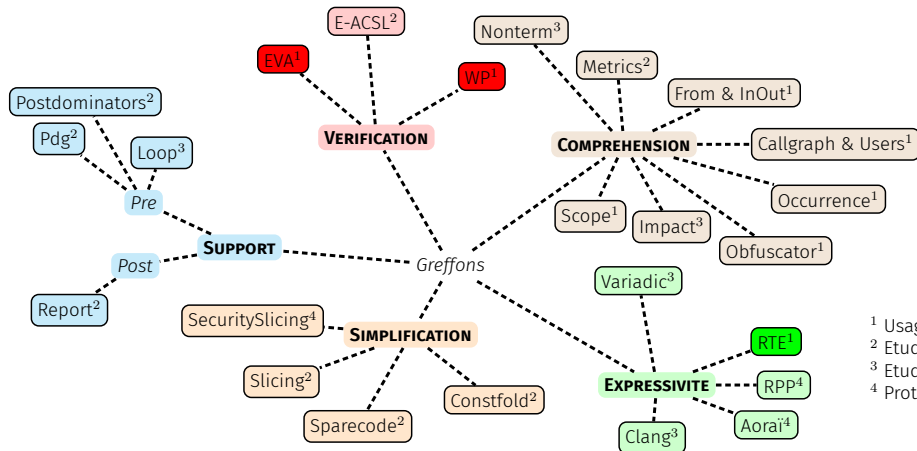


FRAMA-C, PLUS CONCRÈTEMENT

Un schéma vaut mieux qu'un long discours ...

FRAMA-C, PLUS CONCRÈTEMENT

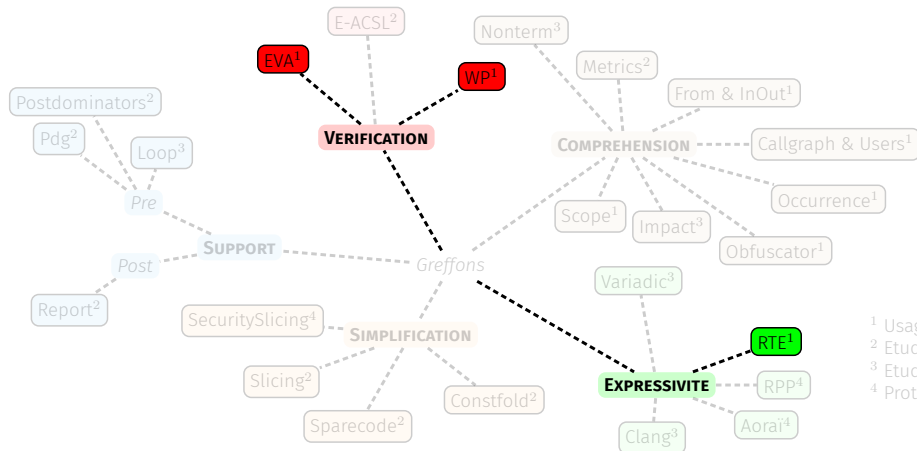
Un schéma vaut mieux qu'un long discours ...



- ¹ Usage industriel
- ² Etude de cas industriel
- ³ Etude de cas interne CEA
- ⁴ Prototype

FRAMA-C, PLUS CONCRÈTEMENT

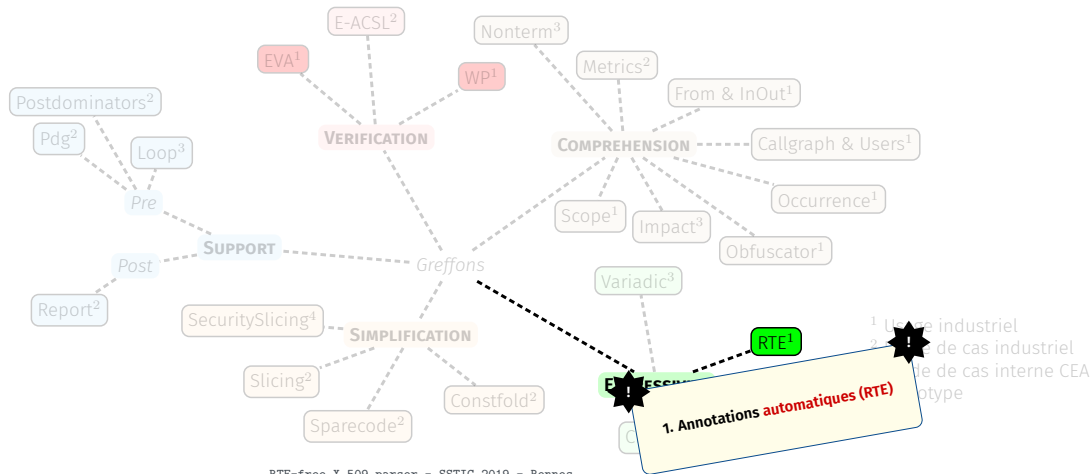
Un schéma vaut mieux qu'un long discours ...



- ¹ Usage industriel
- ² Etude de cas industriel
- ³ Etude de cas interne CEA
- ⁴ Prototype

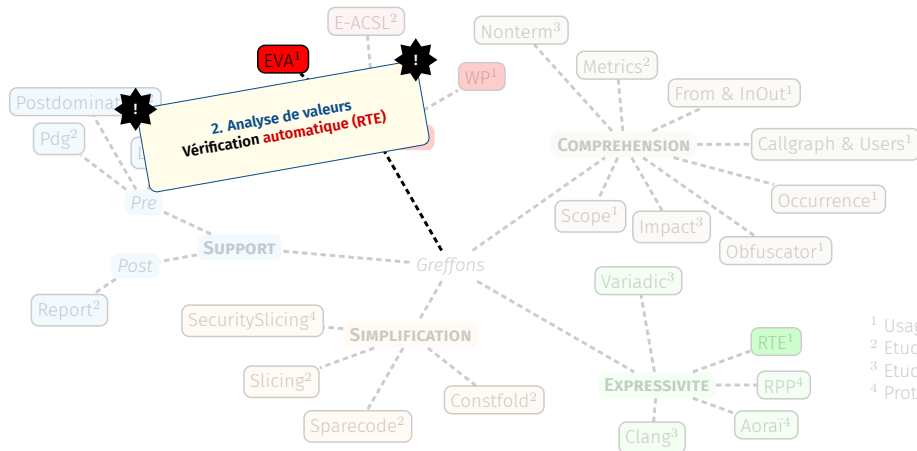
FRAMA-C, PLUS CONCRÈTEMENT

Un schéma vaut mieux qu'un long discours ...



FRAMA-C, PLUS CONCRÈTEMENT

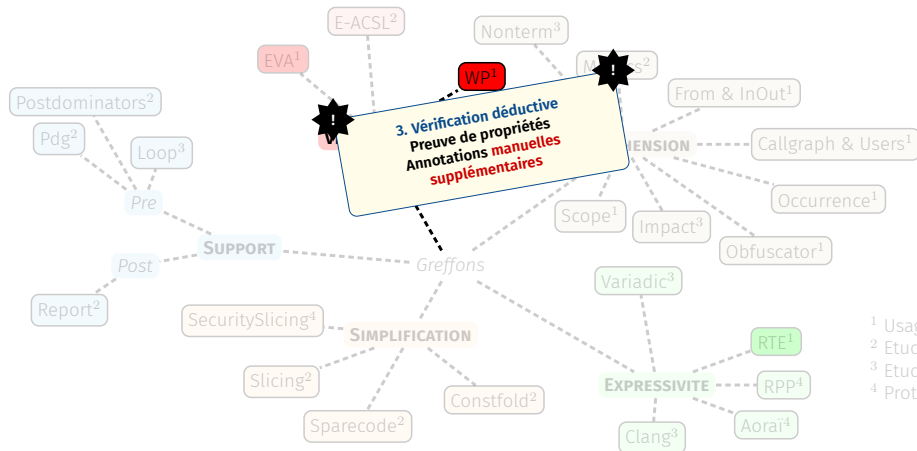
Un schéma vaut mieux qu'un long discours ...



- ¹ Usage industriel
- ² Etude de cas industriel
- ³ Etude de cas interne CEA
- ⁴ Prototype

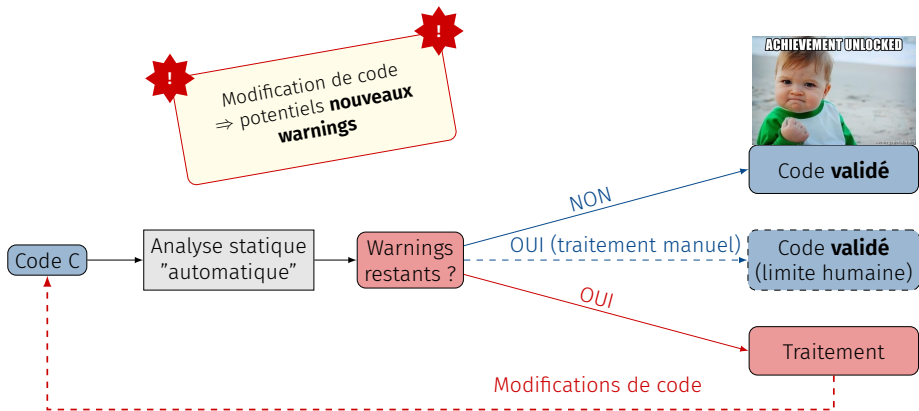
FRAMA-C, PLUS CONCRÈTEMENT

Un schéma vaut mieux qu'un long discours ...

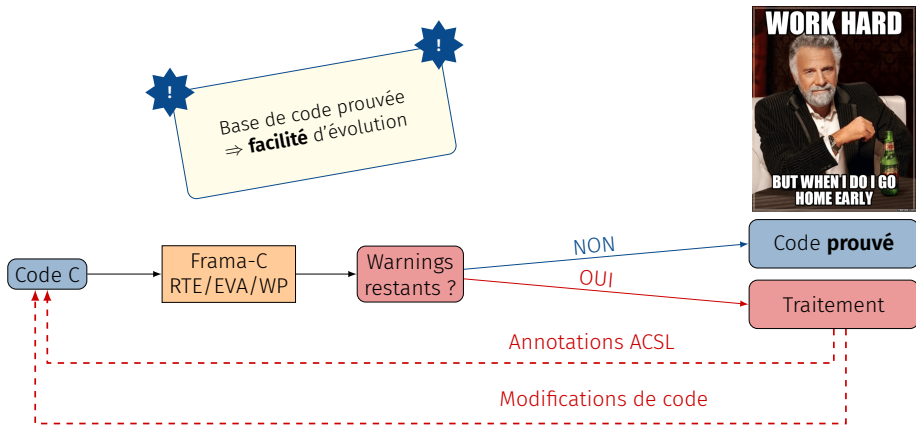


- ¹ Usage industriel
- ² Etude de cas industriel
- ³ Etude de cas interne CEA
- ⁴ Prototype

Workflow D'ANALYSE STATIQUE CLASSIQUE



Workflow AVEC STRATÉGIE EVA/WP



Premier exemple : un contrat de fonction

```
/*
 * Verify given buffer contains only printable characters. negative value is
 * returned on error, 0 on success.
 */
/*@
  @ requires ((len > 0) && (buf != \null)) ==> \valid_read(buf + (0 .. (len - 1)));
  @ ensures (len == 0) || (buf == \null) ==> \result < 0;
  @ assigns \nothing;
  @*/
static int check_printable_string(const u8 *buf, u16 len)
{
    /*...*/
}
```

Deuxième exemple : une boucle

```

static int check_printable_string(const u8 *buf, u16 len)
{
    /*@ loop invariant 0 <= rbytes <= len;
       @ loop assigns rbytes, c, ret;
       @ loop variant (len - rbytes);
       @ */
    for (rbytes = 0; rbytes < len; rbytes++) {
        c = buf[rbytes];
        if ((c >= 'a' && c <= 'z') ||
            (c >= 'A' && c <= 'Z') ||
            (c >= '0' && c <= '9')) {
            continue;
        }
        switch (c) {
            case 39: /* ' */
            case '=':
                /* ... */
            case ' ':
                continue;
            default:
                break;
        }
        ret = -__LINE__;
        ERROR_TRACE_APPEND(__LINE__);
        goto out;
    }
    ret = 0;
out:
    return ret;
}

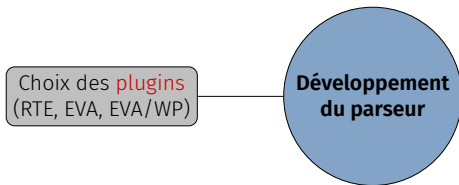
```

ACSL

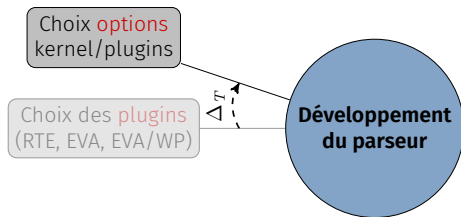
Au final

`requires`, `ensures`, `assigns`, `behavior`, `complete`, `disjoint`, `loop variant`, `loop invariant`, `loop assigns`, `terminates`, `decrease`, `\valid`, `\valid_read`, `\old`, `sets`, `assert`, `\inter`, `\empty`, `\subset`, `\union`, `\at`, `\result`, `type`, `struct`, `logic`, `lemma`, `inductive`, `case`, `axiom`, `axiomatic`, `calls`, `\lambda`, `\match`, `\let`, `==>`, `reads`, `\base_addr`, `\block_length`, `\separated`, `\allocation`, `\offset`, `\allocable`, `\freeable`, `\fresh`, `\valid_function`, `ghost`, `exit`, `breaks`, `continues`, `returns`, `\nothing`, `global invariant`, `type invariant`, `\forall`, `\exists`, `weak`, `strong`, `model`

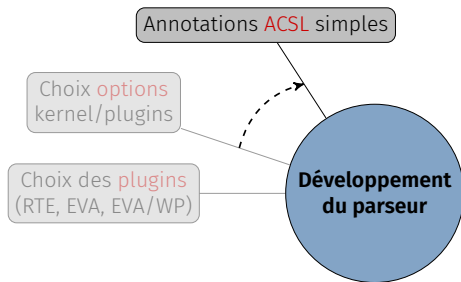
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



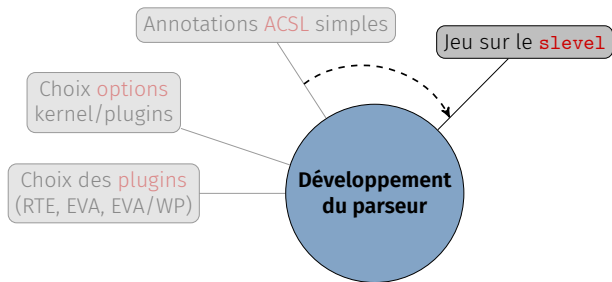
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



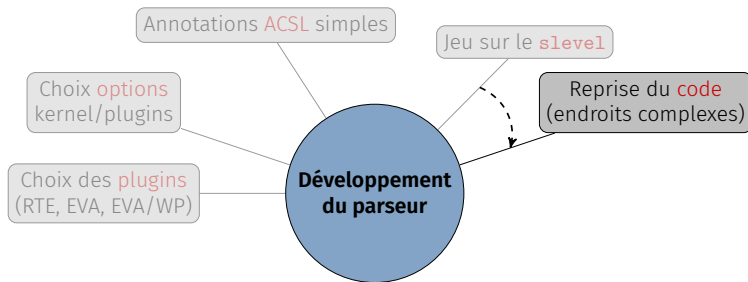
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



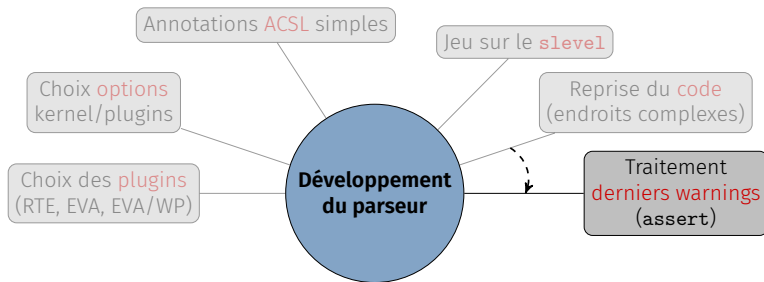
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



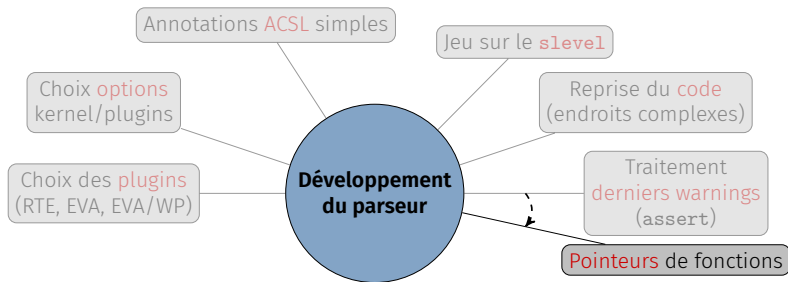
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



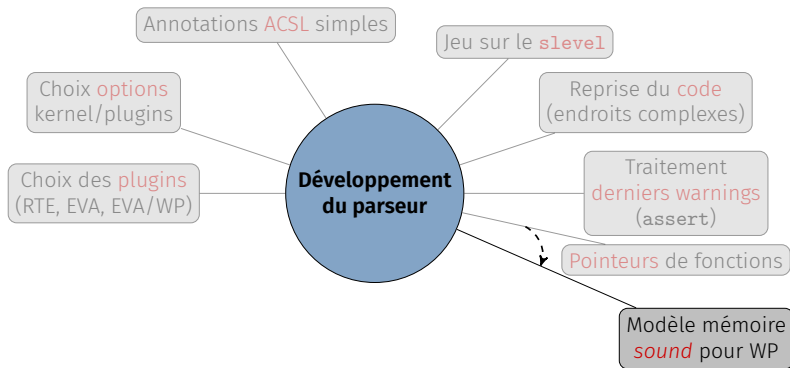
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



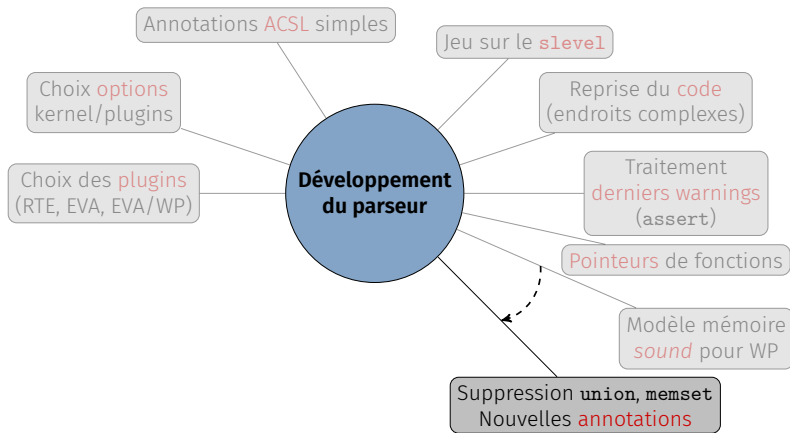
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



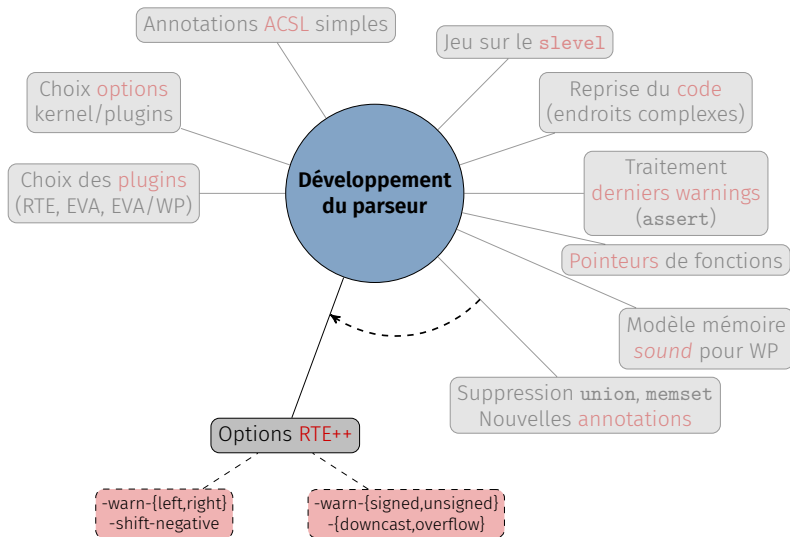
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



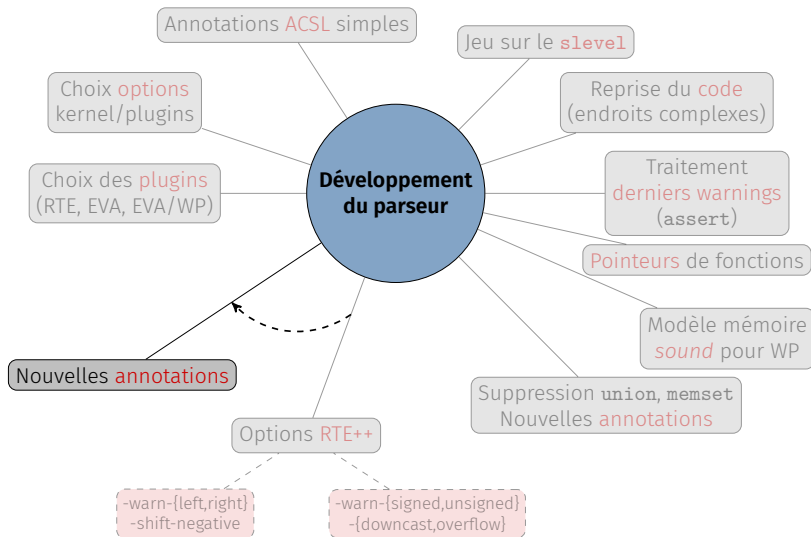
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET

```
$ cat Makefile

JOBS:=$(shell nproc)
SESSION:=frama-c-rte-val-wp.session
TIMEOUT:=15

frama-c:
    frama-c-gui x509_parser.c -machdep x86_64 \
        -warn-left-shift-negative \
        -warn-right-shift-negative \
        -warn-signed-downcast \
        -warn-signed-overflow \
        -warn-unsigned-downcast \
        -warn-unsigned-overflow \
        -rte \
        -eva \
        -eva-slevel 1 \
        -slevel-function="_extract_complex_tag:200, _parse_arc:100, \
            parse_UTCTime:100, find_dn_by_oid:100, \
            find_curve_by_oid:100, find_alg_by_oid:200, \
            find_ext_by_oid:200, parse_AccessDescription:400, \
            parse_x509_Extension:400, parse_x509_subjectPublicKeyInfo:300, \
            parse_x509_Extensions:400, bufs_differ:200, \
            parse_x509_tbsCertificate:400, parse_x509_AlgorithmIdentifier:200" \
        -eva-warn-undefined-pointer-comparison none \
        -then \
        -wp \
        -wp-dynamic \
        -wp-par $(JOBS) \
        -wp-steps 100000 -wp-depth 100000 \
        -wp-split -wp-literals \
        -wp-timeout $(TIMEOUT) -pp-annot -save $(SESSION)
```

RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET

```
$ cat Makefile

JOBS:=$(shell nproc)
SESSION:=frama-c-rte-val-wp.session
TIMEOUT:=15

frama-c:
    frama-c-gui x509_parser.c -machdep x86_64 \
        -warn-left-shift-negative \
        -warn-right-shift-negative \
        -warn-signed-downcast \
        -warn-signed-overflow \
        -warn-unsigned-downcast \
        -warn-unsigned-overflow \
        -rte \
        -eva \
        -eva-slevel 1 \
        -slevel-function="_extract_complex_tag:200, _parse_arc:100, \
            parse_UTCTime:100, find_dn_by_oid:100, \
            find_curve_by_oid:100, find_alg_by_oid:200, \
            find_ext_by_oid:200, parse_AccessDescription:400, \
            parse_x509_Extension:400, parse_x509_subjectPublicKeyInfo:300, \
            parse_x509_Extensions:400, bufs_differ:200, \
            parse_x509_tbsCertificate:400, parse_x509_AlgorithmIdentifier:200" \
        -eva-warn-undefined-pointer-comparison none \
        -then \
        -wp \
        -wp-dynamic \
        -wp-par $(JOBS) \
        -wp-steps 100000 -wp-depth 100000 \
        -wp-split -wp-literals \
        -wp-timeout $(TIMEOUT) -pp-annot -save $(SESSION)
```

RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET

```
$ cat Makefile
```

```
JOBS:=$(shell nproc)
```

```
SESSION:=frama-c-rte-val-wp.session
```

```
TIMEOUT:=15
```

```
frama-c:
```

```
    frama-c-gui x509_parser.c -machdep x86_64 \
        -warn-left-shift-negative \
        -warn-right-shift-negative \
        -warn-signed-downcast \
        -warn-signed-overflow \
        -warn-unsigned-downcast \
        -warn-unsigned-overflow \
        -rte \
        -eva \
        -eva-slevel 1 \
        -slevel-function="_extract_complex_tag:200, _parse_arc:100, \
            parse_UTCTime:100, find_dn_by_oid:100, \
            find_curve_by_oid:100, find_alg_by_oid:200, \
            find_ext_by_oid:200, parse_AccessDescription:400, \
            parse_x509_Extension:400, parse_x509_subjectPublicKeyInfo:300, \
            parse_x509_Extensions:400, bufs_differ:200, \
            parse_x509_tbsCertificate:400, parse_x509_AlgorithmIdentifier:200" \
        -eva-warn-undefined-pointer-comparison none \
        -then \
        -wp \
        -wp-dynamic \
        -wp-par $(JOBS) \
        -wp-steps 100000 -wp-depth 100000 \
        -wp-split -wp-literals \
        -wp-timeout $(TIMEOUT) -pp-annot -save $(SESSION)
```

RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET

```
$ cat Makefile

JOBS:=$(shell nproc)
SESSION:=frama-c-rte-val-wp.session
TIMEOUT:=15

frama-c:
    frama-c-gui x509_parser.c -machdep x86_64 \
        -warn-left-shift-negative \
        -warn-right-shift-negative \
        -warn-signed-downcast \
        -warn-signed-overflow \
        -warn-unsigned-downcast \
        -warn-unsigned-overflow \
        -rte \
        -eva \
        -eva-slevel 1 \
        -slevel-function="_extract_complex_tag:200, _parse_arc:100, \
            parse_UTCTime:100, find_dn_by_oid:100, \
            find_curve_by_oid:100, find_alg_by_oid:200, \
            find_ext_by_oid:200, parse_AccessDescription:400, \
            parse_x509_Extension:400, parse_x509_subjectPublicKeyInfo:300, \
            parse_x509_Extensions:400, bufs_differ:200, \
            parse_x509_tbsCertificate:400, parse_x509_AlgorithmIdentifier:200" \
        -eva-warn-undefined-pointer-comparison none \
        -then \
        -wp \
        -wp-dynamic \
        -wp-par $(JOBS) \
        -wp-steps 100000 -wp-depth 100000 \
        -wp-split -wp-literals \
        -wp-timeout $(TIMEOUT) -pp-annot -save $(SESSION)
```

RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET

```
$ cat Makefile

JOBS:=$(shell nproc)
SESSION:=frama-c-rte-val-wp.session
TIMEOUT:=15

frama-c:
    frama-c-gui x509_parser.c -machdep x86_64 \
        -warn-left-shift-negative \
        -warn-right-shift-negative \
        -warn-signed-downcast \
        -warn-signed-overflow \
        -warn-unsigned-downcast \
        -warn-unsigned-overflow \
        -rte \
        -eva \
        -eva-slevel 1 \
        -slevel-function="_extract_complex_tag:200, _parse_arc:100, \
            parse_UTCTime:100, find_dn_by_oid:100, \
            find_curve_by_oid:100, find_alg_by_oid:200, \
            find_ext_by_oid:200, parse_AccessDescription:400, \
            parse_x509_Extension:400, parse_x509_subjectPublicKeyInfo:300, \
            parse_x509_Extensions:400, bufs_differ:200, \
            parse_x509_tbsCertificate:400, parse_x509_AlgorithmIdentifier:200" \
        -eva-warn-undefined-pointer-comparison none \
        -then \
        -wp \
        -wp-dynamic \
        -wp-par $(JOBS) \
        -wp-steps 100000 -wp-depth 100000 \
        -wp-split -wp-literals \
        -wp-timeout $(TIMEOUT) -pp-annot -save $(SESSION)
```

RETEX FRAMA-C : QUELQUES STATISTIQUES

≈3000 SLOC de C (hors commentaires)

- 35 boucles, 516 goto
- 249 déréférencements de pointeurs
- 100 fonctions, 126 pointeurs de fonctions, 36 fonctions pointées

RETEX FRAMA-C : QUELQUES STATISTIQUES

≈3000 SLOC de C (hors commentaires)

- 35 boucles, 516 goto
- 249 déréférencements de pointeurs
- 100 fonctions, 126 pointeurs de fonctions, 36 fonctions pointées

≈1000 annotations ACSL **manuelles**

- 114 annotations de boucles (≈ 3.5 annotations par boucle)
- 83 **assert**
- Contrats de fonctions (≈ 8 annotations par contrat):
 - ➡ **ensures** 342 (≈ 3.5 par fonction)
 - ➡ **assigns** 98 (≈ 1 par fonction)
 - ➡ **requires** 343 (≈ 3.5 par fonction)
- 5 annotations **calls**

RETEX FRAMA-C : POINTEURS DE FONCTION

```
static int parse_x509_AlgorithmIdentifier(
    const u8 *buf, u16 len,
    const alg_id **alg,
    alg_param *param, u16 *eaten)
{
    const alg_id *talg = NULL;
    u16 hdr_len = 0;
    u16 data_len = 0;
    u16 param_len;
    u16 oid_len = 0;
    int ret;
```

```
/* requires len >= 0;
 * requires ((len > 0) && (buf != NULL)) ==>
 *   \valid_read(buf + (0 .. (len - 1)));
 * ensures (\result != NULL) ==>
 *   \exists integer i; 0 <= i < NUM_KNOWN_ALGS &&
 *     \result == known_algs[i];
 * ensures (len == 0) ==> \result == NULL;
 * ensures (buf == NULL) ==> \result == NULL;
 * assigns \nothing; */
static const alg_id *find_alg_by_oid(const u8 *buf, u16 len)
```

```
typedef struct {
    const u8 *alg_name;
    const u8 *alg_printable_oid;
    const u8 *alg_der_oid;
    const u8 alg_der_oid_len;
    const u8 alg_type;
    int (*parse_sig)(const u8 *buf, u16 len, u16 *eaten);
    int (*parse_subjectpubkey)(const u8 *buf, u16 len, alg_param *param);
    int (*parse_algid_params)(const u8 *buf, u16 len, alg_param *param);
} _alg_id;
```

AlgorithmIdentifier ::= SEQUENCE {
 algorithm
 parameters
 OBJECT IDENTIFIER,
 ANY DEFINED BY algorithm OPTIONAL
}

```
ret = talg->parse_algid_params(buf, param_len, param);
if (ret) {
    ERROR_TRACE_APPEND(_LINE_);
    goto out;
}

*alg = talg;
*eaten = hdr_len + data_len;

ret = 0;

out:
return ret;
}
```

```
/* assert \valid_read(buf + (0 .. (len - 1))); */
ret = !bufs_differ(cur->alg_der_oid, buf,
                  cur->alg_der_oid_len);
if (ret) {
    found = cur;
    break;
}
}
out:
return found;
}
```

```
...
    &ecdsa_sha256_alg,
    ...
#ifdef TEMPORARY_BADALGS
    &rsa_md2_alg,
    ...
#endif
};

#define NUM_KNOWN_ALGS (sizeof(known_algs) / sizeof(known_algs[0]))
```

RETEX FRAMA-C : POINTEURS DE FONCTION

```

static int parse_x509_AlgorithmIdentifier(
    const u8 *buf, u16 len,
    const _alg_id **alg,
    alg_param *param, u16 *eaten)
{
    const _alg_id *talg = NULL;
    u16 hdr_len = 0;
    u16 data_len = 0;
    u16 param_len;
    u16 oid_len = 0;
    int ret;

    ...

    ret = parse_OID(buf, data_len, &oid_len);
    if (ret) {
        ERROR_TRACE_APPEND(_LINE_);
        goto out;
    }

    talg = find_alg_by_oid(buf, oid_len);
    if (talg == NULL) {
        ret = _LINE_;
        ERROR_TRACE_APPEND(_LINE_);
        goto out;
    }

    ...

    /* calls parse_algid_params_generic,
       parse_algid_params_ecdsa_with,
       parse_algid_params_ecPublicKey,
       parse_algid_params_rsa; */
    ret = talg->parse_algid_params(buf, param_len, param);
    if (ret) {
        ERROR_TRACE_APPEND(_LINE_);
        goto out;
    }

    *alg = talg;
    *eaten = hdr_len + data_len;

    ret = 0;

out:
    return ret;
}

```

/* requires len >= 0;
 * requires ((len > 0) && (buf != NULL)) ==>
 * \valid_read(buf + (0 .. (len - 1)));
 *
 * ensures (\result != NULL) ==>
 * \exists integer i; 0 <= i < NUM_KNOWN_ALGS &&
 * \result == known_algs[i];
 *
 * ensures (len == 0) ==> \result == NULL;
 * ensures (buf == NULL) ==> \result == NULL;
 * assigns \nothing; */
static const _alg_id * find_alg_by_oid(const u8 *buf, u16 len)
{
 const _alg_id *found = NULL;
 const _alg_id *cur = NULL;
 u8 k;

 ...

 /* loop invariant 0 <= k <= NUM_KNOWN_ALGS;
 * loop invariant found == NULL;
 * loop assigns cur, found, k;
 * loop variant (NUM_KNOWN_ALGS - k); */
 for (k = 0; k < NUM_KNOWN_ALGS; k++) {
 int ret;

 cur = known_algs[k];

 /* assert cur == known_algs[k]; */
 if (cur->alg_der_oid_len != len) {
 continue;
 }

 /* assert \valid_read(buf + (0 .. (len - 1))); */
 ret = !bufs_differ(cur->alg_der_oid, buf,
 cur->alg_der_oid_len);

 if (ret) {
 found = cur;
 break;
 }
 }

 out:
 return found;
}

```

typedef struct {
    const u8 *alg_name;
    const u8 *alg_printable_oid;
    const u8 *alg_der_oid;
    const u8 alg_der_oid_len;
    const u8 alg_type;
    int (*parse_sig)(const u8 *buf, u16 len, u16 *eaten);
    int (*parse_subjectpubkey)(const u8 *buf, u16 len, alg_param *param);
    int (*parse_algid_params)(const u8 *buf, u16 len, alg_param *param);
} _alg_id;

...

static const u8 _ecdsa_sha256_name[] = "ecdsa-with-SHA256";
static const u8 _ecdsa_sha256_printable_oid[] = "1.2.840.10045.4.3.2";
static const u8 _ecdsa_sha256_der_oid[] = {
    0x06, 0x08, 0x2a, 0x86, 0x48,
    0xce, 0x3d, 0x04, 0x03, 0x02 };

static const _alg_id _ecdsa_sha256_alg = {
    .alg_name = _ecdsa_sha256_name,
    .alg_printable_oid = _ecdsa_sha256_printable_oid,
    .alg_der_oid = _ecdsa_sha256_der_oid,
    .alg_der_oid_len = sizeof(_ecdsa_sha256_der_oid),
    .alg_type = ALG_SIG,
    .parse_sig = parse_sig_ecdsa,
    .parse_subjectpubkey = NULL,
    .parse_algid_params = parse_algid_params_ecdsa_with,
};

...

static const _alg_id *known_algs[] = {

    ...

    &_ecdsa_sha256_alg,

    ...

#ifdef TEMPORARY_BADALGS
    &_rsa_md2_alg,

    ...
#endif
};

#define NUM_KNOWN_ALGS (sizeof(known_algs) / sizeof(known_algs[0]))

```

RETEX FRAMA-C : POINTEURS DE FONCTION

```

static int parse_x509_AlgorithmIdentifier(
    const u8 *buf, u16 len,
    const _alg_id **alg,
    alg_param *param, u16 *eaten)
{
    const _alg_id *talg = NULL;
    u16 hdr_len = 0;
    u16 data_len = 0;
    u16 param_len;
    u16 oid_len = 0;
    int ret;

    ...

    ret = parse_OID(buf, data_len, &oid_len);
    if (ret) {
        ERROR_TRACE_APPEND(_LINE_);
        goto out;
    }

    talg = find_alg_by_oid(buf, oid_len);
    if (talg == NULL) {
        ret = _LINE_;
        ERROR_TRACE_APPEND(_LINE_);
        goto out;
    }

    ...

    /* calls parse_algid_params_generic,
       parse_algid_params_ecdsa_with,
       parse_algid_params_ecPublicKey,
       parse_algid_params_rsa; */
    ret = talg->parse_algid_params(buf, param_len, param);
    if (ret) {
        ERROR_TRACE_APPEND(_LINE_);
        goto out;
    }

    *alg = talg;
    *eaten = hdr_len + data_len;

    ret = 0;

out:
    return ret;
}

```

/* requires len >= 0;
 * requires ((len > 0) && (buf != NULL)) ==>
 * \valid_read(buf + (0 .. (len - 1)));
 * ensures (\result != NULL) ==>
 * \exists integer i; 0 <= i < NUM_KNOWN_ALGS &&
 * \result == known_algs[i];
 * ensures (len == 0) ==> \result == NULL;
 * ensures (buf == NULL) ==> \result == NULL;
 * assigns \nothing; */
static const _alg_id * find_alg_by_oid(const u8 *buf, u16 len)
{
 const _alg_id *found = NULL;
 const _alg_id *cur = NULL;
 u8 k;

 ...

 /* loop invariant 0 <= k <= NUM_KNOWN_ALGS;
 * loop invariant found == NULL;
 * loop assigns cur, found, k;
 * loop variant (NUM_KNOWN_ALGS - k); */
 for (k = 0; k < NUM_KNOWN_ALGS; k++) {
 int ret;

 cur = known_algs[k];

 /* assert cur == known_algs[k]; */
 if (cur->alg_der_oid_len != len) {
 continue;
 }

 /* assert \valid_read(buf + (0 .. (len - 1))); */
 ret = !bufs_differ(cur->alg_der_oid, buf,
 cur->alg_der_oid_len);

 if (ret) {
 found = cur;
 break;
 }
 }

 out:
 return found;
}

```

typedef struct {
    const u8 *alg_name;
    const u8 *alg_printable_oid;
    const u8 *alg_der_oid;
    const u8 alg_der_oid_len;
    const u8 alg_type;
    int (*parse_sig)(const u8 *buf, u16 len, u16 *eaten);
    int (*parse_subjectpubkey)(const u8 *buf, u16 len, alg_param *param);
    int (*parse_algid_params)(const u8 *buf, u16 len, alg_param *param);
} _alg_id;

...

static const u8 _ecdsa_sha256_name[] = "ecdsa-with-SHA256";
static const u8 _ecdsa_sha256_printable_oid[] = "1.2.840.10045.4.3.2";
static const u8 _ecdsa_sha256_der_oid[] = {
    0x06, 0x08, 0x2a, 0x86, 0x48,
    0xce, 0x3d, 0x04, 0x03, 0x02 };

static const _alg_id _ecdsa_sha256_alg = {
    .alg_name = _ecdsa_sha256_name,
    .alg_printable_oid = _ecdsa_sha256_printable_oid,
    .alg_der_oid = _ecdsa_sha256_der_oid,
    .alg_der_oid_len = sizeof(_ecdsa_sha256_der_oid),
    .alg_type = ALG_SIG,
    .parse_sig = parse_sig_ecdsa,
    .parse_subjectpubkey = NULL,
    .parse_algid_params = parse_algid_params_ecdsa_with,
};

...

static const _alg_id *known_algs[] = {

    ...

    &_ecdsa_sha256_alg,

    ...

#ifdef TEMPORARY_BADALGS
    &_rsa_md2_alg,

    ...
#endif
};

#define NUM_KNOWN_ALGS (sizeof(known_algs) / sizeof(known_algs[0]))

```

RETEX FRAMA-C : POINTEURS DE FONCTION

[parse_sig_generic](#)
[parse_subjectpubkey_ec](#)
[parse_subjectpubkey_rsa](#)
[parse_Time](#)
[parse_UserNotice](#)
[parse_UTCTime](#)
[parse_x509_AlgorithmIdentifier](#)
[parse_x509_cert](#)
[parse_x509_Extension](#)
[parse_x509_Extensions](#)
[parse_x509_Name](#)
[parse_x509_signatureAlgorithm](#)
[parse_x509_signatureValue](#)
[parse_x509_subjectPublicKeyInfo](#)
[parse_x509_tbsCertificate](#)
[parse_x509_Validity](#)
[parse_x509_Version](#)

WP
 Model... Typed
 Script... (None)
 Provers... Alt-Ergo (native)
☐ RTE ☒ Split ☐ Trace
 Steps 100000
 Depth 100000
 Timeout 15
 Process 4
Occurrence
 Current var None

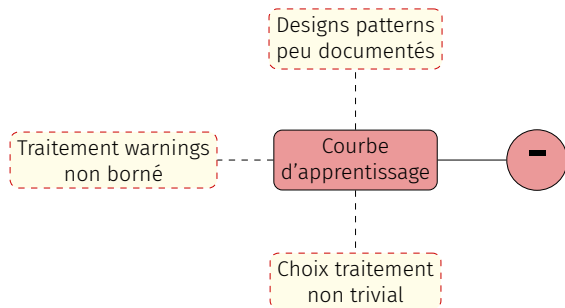
```

/* preconditions of parse_algoid_params_rsa:
requires param_len ≥ 0;
requires
  param_len > 0 ∧ buf ≠ \null ⇒
    \valid_read(buf + (0 .. param_len - 1));
requires param ≠ \null ⇒ \valid_read(param);
preconditions of parse_algoid_params_generic:
requires param_len ≥ 0;
requires
  param_len > 0 ∧ buf ≠ \null ⇒
    \valid_read(buf + (0 .. param_len - 1));
requires param ≠ \null ⇒ \valid_read(param);
preconditions of parse_algoid_params_ecPublicKey:
requires param_len ≥ 0;
requires
  param_len > 0 ∧ buf ≠ \null ⇒
    \valid_read(buf + (0 .. param_len - 1));
requires \valid(param);
requires \separated(param, buf + (..));
preconditions of parse_algoid_params_ecdsa_with:
requires param_len ≥ 0;
requires
  param_len > 0 ∧ buf ≠ \null ⇒
    \valid_read(buf + (0 .. param_len - 1));
requires \valid(param);
requires \separated(param, buf + (..)); */
/*@ assert rte: mem_access: \valid_read(&talg->parse_algoid_params); */
/*@ assert
  rte: function_pointer: \valid_function(talg->parse_algoid_params);
*/
/*@ calls parse_algoid_params_generic, parse_algoid_params_ecdsa_with,
  parse_algoid_params_ecPublicKey, parse_algoid_params_rsa;
*/
ret = (*(talg->parse_algoid_params))(buf,param_len,param);
if (ret) {
  goto out;
}
/*@ assert rte: mem_access: \valid(alg); */
*alg = talg;
  
```

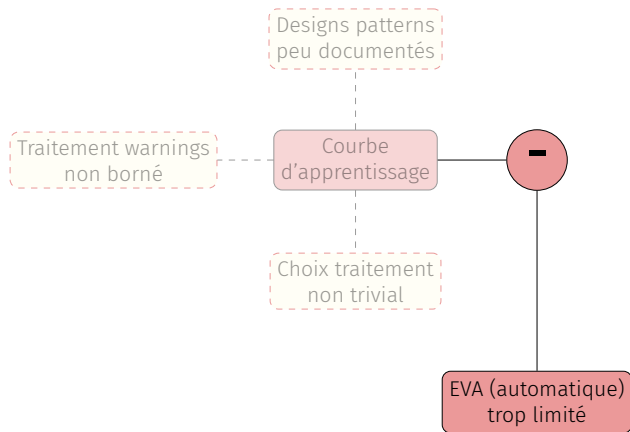
RETEX FRAMA-C : L'OUTIL



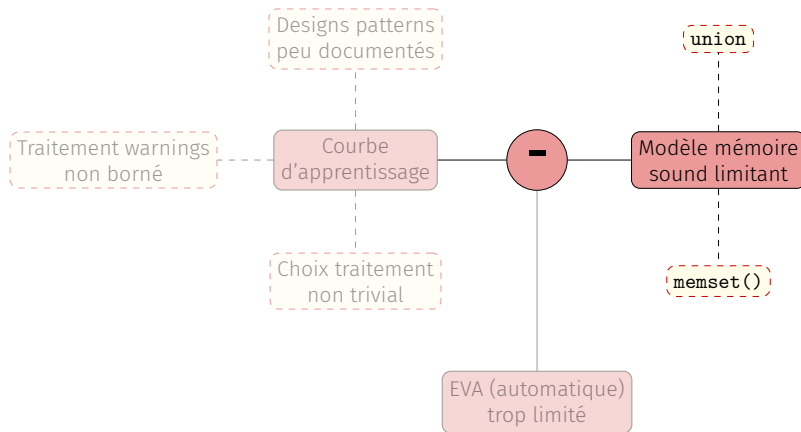
RETEX FRAMA-C : L'OUTIL



RETEX FRAMA-C : L'OUTIL



RETEX FRAMA-C : L'OUTIL



RETEX FRAMA-C : L'OUTIL

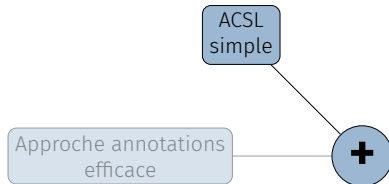


RETEX FRAMA-C : L'OUTIL

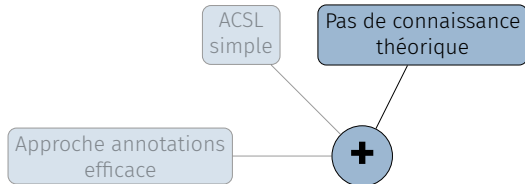
Approche annotations
efficace



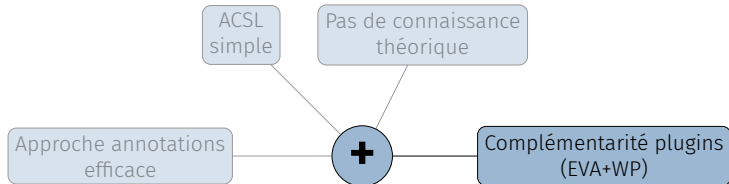
RETEX FRAMA-C : L'OUTIL



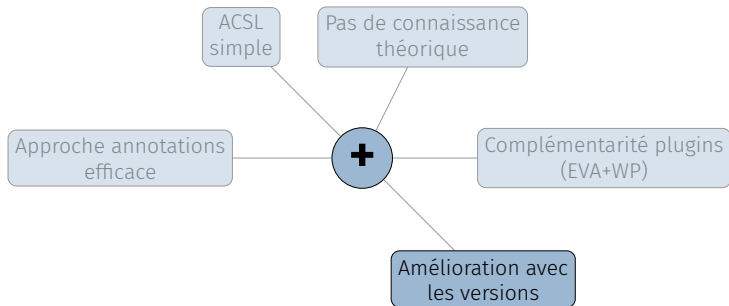
RETEX FRAMA-C : L'OUTIL



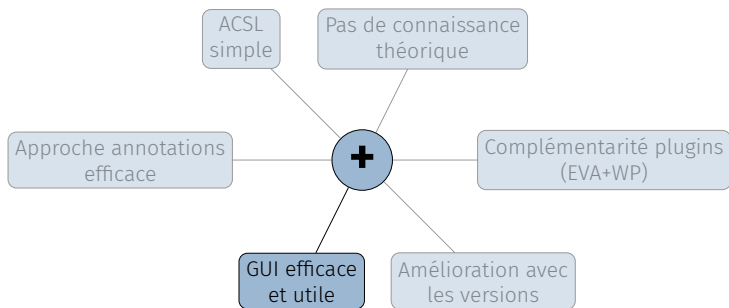
RETEX FRAMA-C : L'OUTIL



RETEX FRAMA-C : L'OUTIL



RETEX FRAMA-C : L'OUTIL



AUTRES STRATÉGIE ET OUTILS

Stratégie sound et automatique de vérification

EVA (Frama-C)	58 warnings	185s
CodeProver (MathWorks)	50 warnings	207s

Fausse alarmes sur accès mémoire

AUTRES STRATÉGIE ET OUTILS

Stratégie sound et automatique de vérification

EVA (Frama-C)	58 warnings	185s
CodeProver (MathWorks)	50 warnings	207s

Fausse alarmes sur accès mémoire

Plus d'outils pour plus de vues différentes

Outils orientés défauts de code

BugFinder (MathWorks)	44 défauts	<60 s
Coverity (Synopsis)	31 défauts	<60 s

Identification d'un bug logique !

BUG LOGIQUE (COMMENT ACCEPTER 285234 CERTIFICATS INVALIDES)

```
diff --git a/src/x509_parser.c b/src/x509_parser.c
@@ -5578,12 +5578,14 @@ static int parse_DisplayText(const u8 *buf, u16
    len, u16 *eaten)
    {
        case STR_TYPE_BMP_STRING:
            ret = check_bmp_string(buf, data_len);
            if (ret) {
                ERROR_TRACE_APPEND(__LINE__);
+               goto out;
            }
            break;
        default:
            ret = -__LINE__;
            ERROR_TRACE_APPEND(__LINE__);
+            goto out;
            break;
    }

@@ -5614,7 +5619,6 @@ static int parse_DisplayText(const u8 *buf, u16
    len, u16 *eaten)
    {
        break;
    }

-    ret = 0;
out:
    return ret;
}
```

STATUT

- Parseur (syntaxique) de certificats X.509
 - ➡ Garanti **sans RTE**
 - ➡ **Utilisable** pour :
 - ▶ implémentation fonctionnelle,
 - ▶ triage/validation (sur une sonde, ...),
 - ▶ ...
- Code **annoté** :
 - ➡ disponible (<https://github.com/ANSSI-FR/x509-parser>),
 - ➡ outil de validation Frama-C **Open Source**
- Pour le **développeur** :
 - ➡ validation des **évolutions possibles**,
 - ➡ **exemples** de *design pattern* annotés
- À venir : **finalisation**, **signatures**, **bugs logiques**, **AFL**, ...

[illegible]

À VENIR

- Finalisation de l'implémentation (documentation ;-)
- Implémentation de la validation de signature (avec libecc)
- Travail sur les bugs logiques
- Test d'autres outils sur la base de code (AFL sur le set de certificats)
- Version longue de l'article avec plus de détails

DES MODÈLES MÉMOIRE "SOUND" (TYPED_CAST_REF VS TYPED)

```
diff --git a/src/x509_parser.c b/src/x509_parser.c
--- a/src/x509_parser.c
+++ b/src/x509_parser.c
@@ -8427,5 +8454,13 @@ static int parse_x509_tbsCertificate(const u8 *
    buf, u16 len,
        goto out;
    }

-    memset(&ctx, 0, sizeof(ctx));
+    ctx.empty_subject = 0;
+    ctx.ca_true = 0;
+    ctx.bc_critical = 0;
+    ctx.has_ski = 0;
+    ctx.has_keyUsage = 0;
+    ctx.keyCertSign_set = 0;
+    ctx.has_name_constraints = 0;
+    ctx.has_crldp = 0;
+    ctx.self_signed = 0;
```

DES MODÈLES MÉMOIRE "SOUND" (TYPED_CAST_REF VS TYPED)

```
diff --git a/src/x509_parser.c b/src/x509_parser.c
--- a/src/x509_parser.c
+++ b/src/x509_parser.c
@@ -1114,9 +1114,10 @@ typedef struct {
     const u16 crv_order_bit_len;
 } _curve;

-typedef union {
-    const _curve *curve_param;
-    const u8 *null_param;
-    const void *no_param;
+typedef struct {
+    const _curve *curve_param;
+    const u8 *null_param;
+    int ecdsa_no_param;
+    int unparsed_param;
 } alg_param;
```

DÉFAUTS : PLUS DE DÉTAILS

	Coverity	BugFinder	fichier(s) concerné(s)
Version	2019.03	2.6	-
Temps analyse	<60s	<60s	
Nombre de défauts	31	44	main.c & x509_parser.c
Code mort	4 (12.9%)	2 (4.6%)	x509_parser.c
Code non atteignable (condition false)	-	3 (6.8%)	main.c & x509_parser.c
Type énuméré mixé avec autre type	2 (4.6%)	-	x509_parser.c
Resource leak	1 (3.2%)	-	main.c
Stack use	1 (3.2%)	-	main.c
Unused value	23 (74.3%)	28 (63.6%)	x509_parser.c
Borne de boucle en dur	-	5 (11.4%)	x509_parser.c
Condition toujours vraie dans if	-	4 (9.1%)	x509_parser.c
Retour de fonction sensible non lue		1 (2.3%)	main.c
Manipulation d'un chemin vulnérable		1 (2.3%)	main.c