Journey to a RTE-free X.509 parser

(with Frama-C)

{LRP,LSL,LSC}

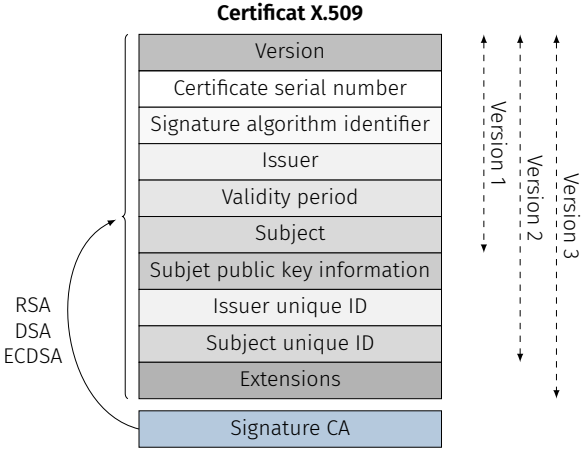
ANSSI

prenom.nom@ssi.gouv.fr

6 juin 2019

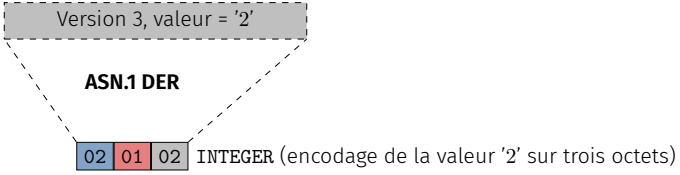
X.509 : BIENVENUE EN ENFER

- X.509 : format d'encodage des certificats



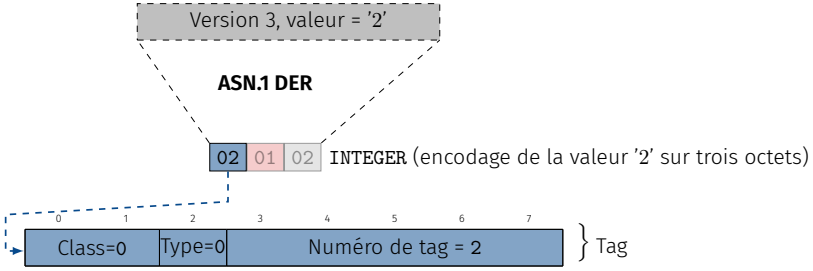
X.509 : BIENVENUE EN ENFER

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



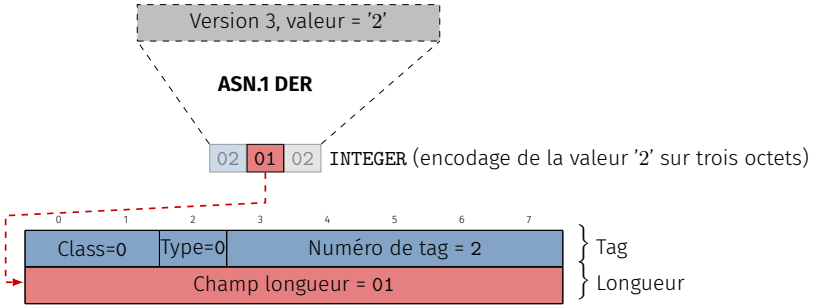
X.509 : BIENVENUE EN ENFER

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



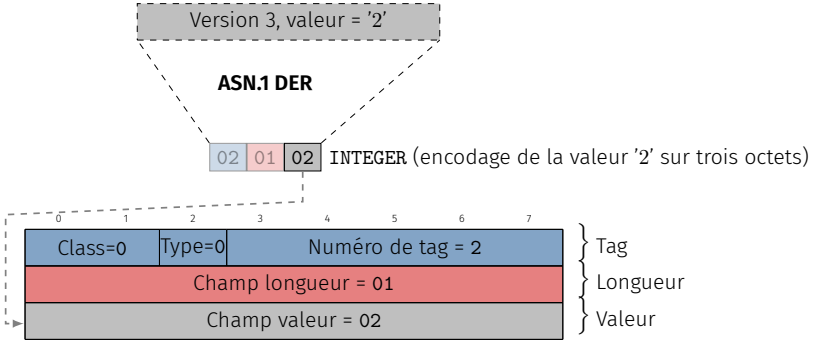
X.509 : BIENVENUE EN ENFER

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

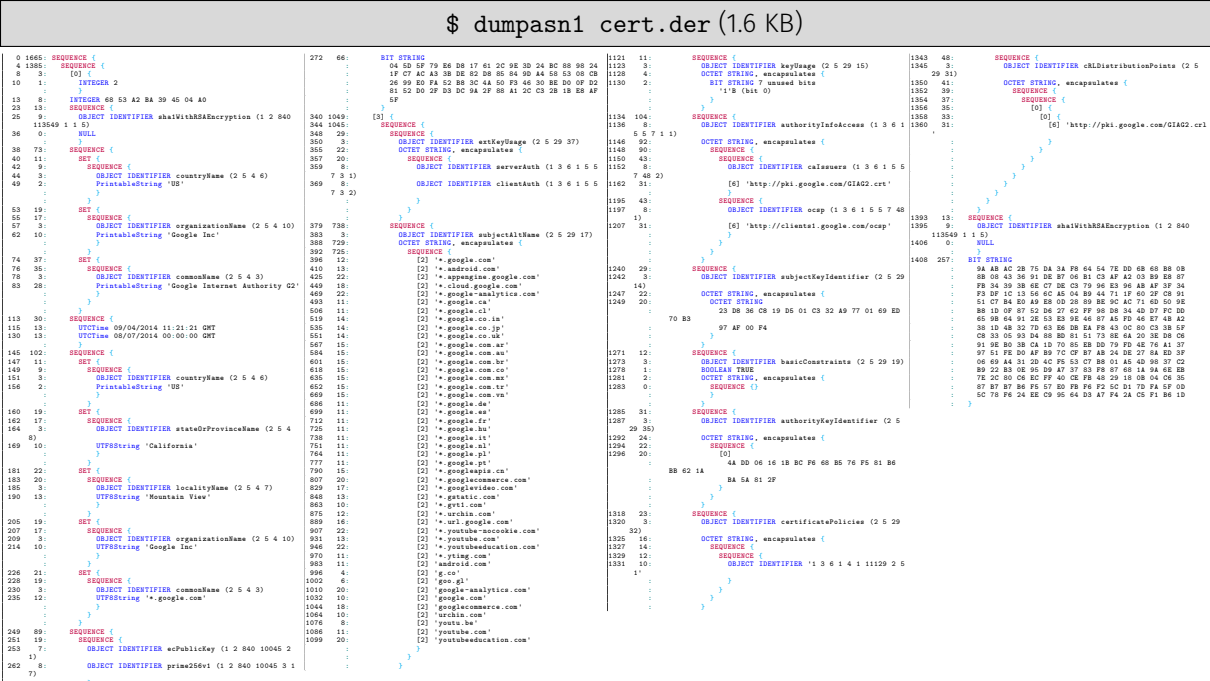


X.509 : BIENVENUE EN ENFER

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

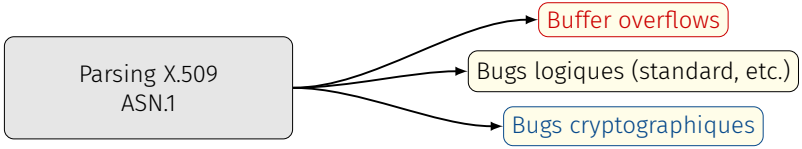


$ dumpasn1 cert.der (1.6 KB)



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

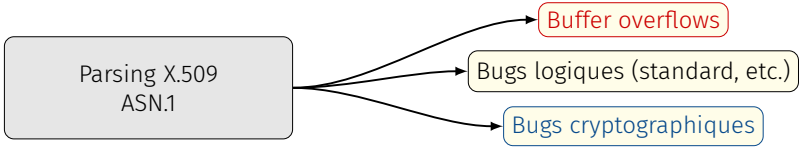
Complexité induit vulnérabilité



Paradoxal pour une brique censée amener de la sécurité !

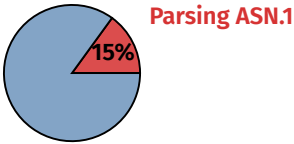
X.509/ASN.1 : YOUR CVE PROVIDER SINCE 1999

Complexité induit vulnérabilité



Paradoxal pour une brique censée amener de la sécurité !

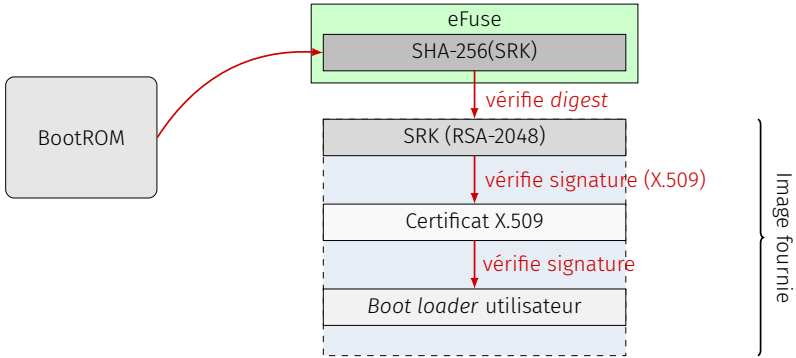
CVE OpenSSL depuis 1999 :



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

CVE-2017-7932

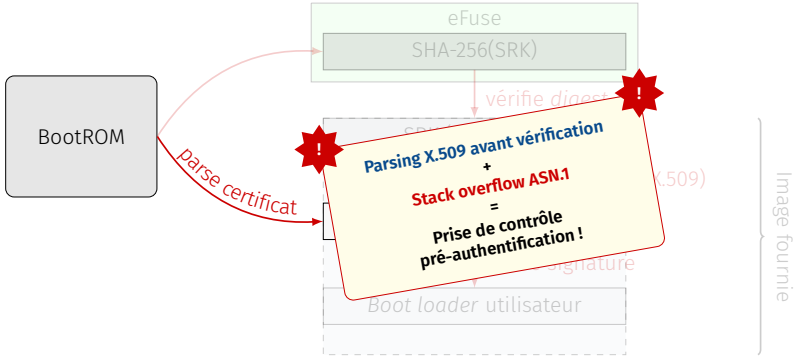
HAB (*High Assurance Boot*) des SoC i.MX28 à i.MX7 compromis (BootROM, irréversible)



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

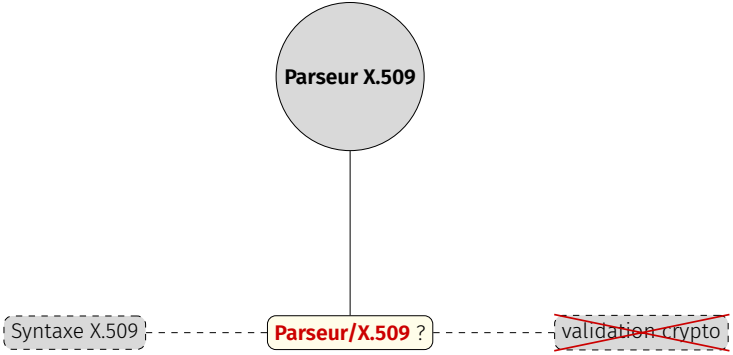
CVE-2017-7932

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

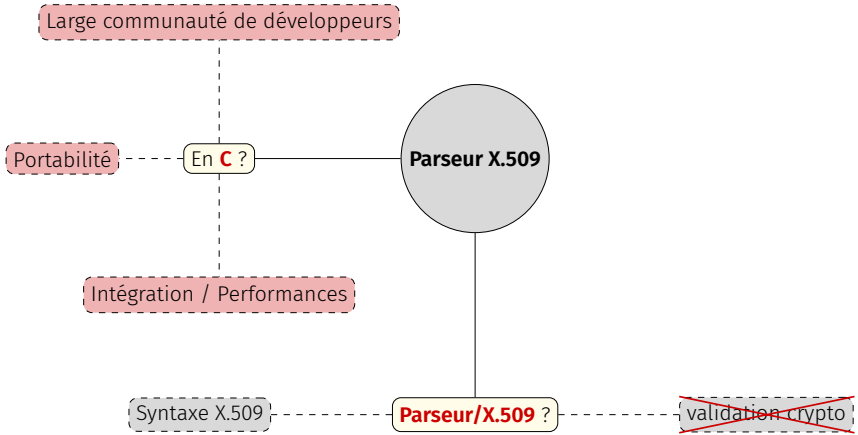


Un parseur X.509 en C "propre" ?

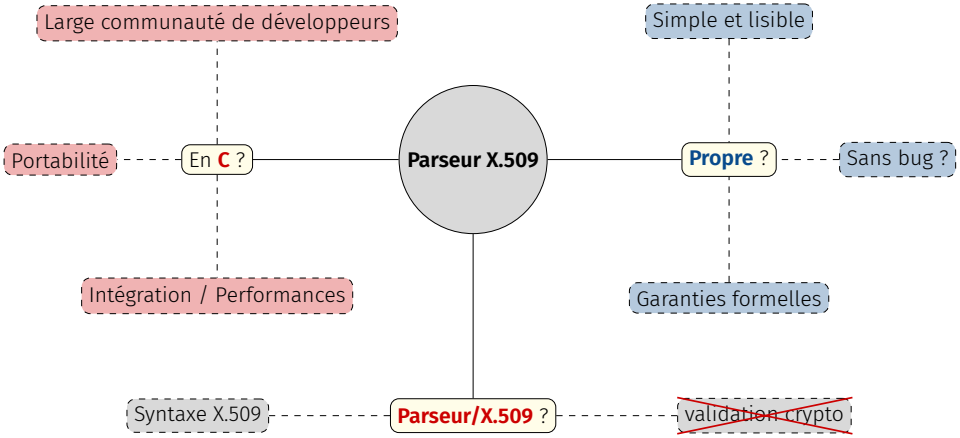
Un parseur X.509 en C "propre" ?



Un parseur X.509 en C "propre" ?

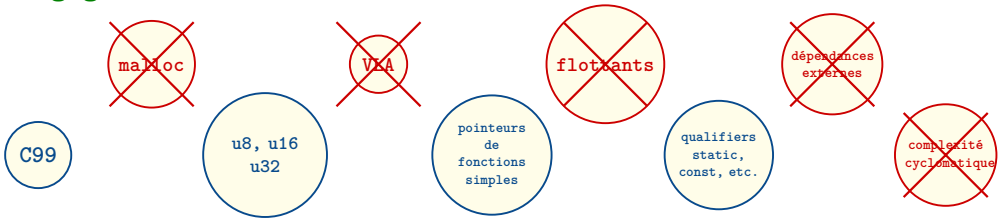


Un parseur X.509 en C "propre" ?



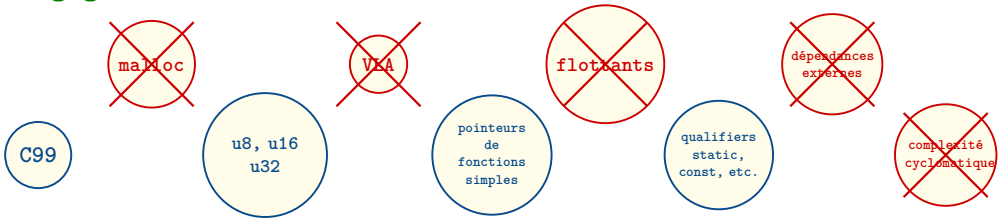
Développement

Langage C



Développement

Langage C

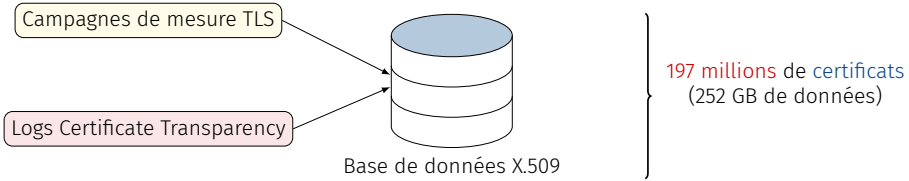


options de compilation strictes

```
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
```

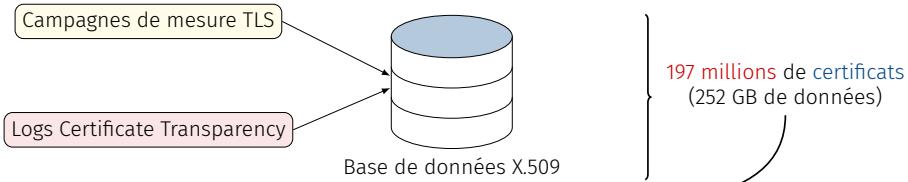
DATA SET

Origine et contenu



Data set

Origine et contenu

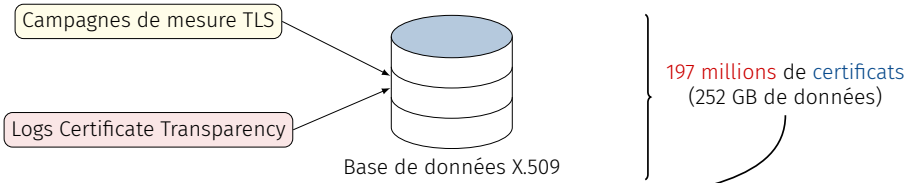


Intérêts

Décisions d'implémentation

Data set

Origine et contenu



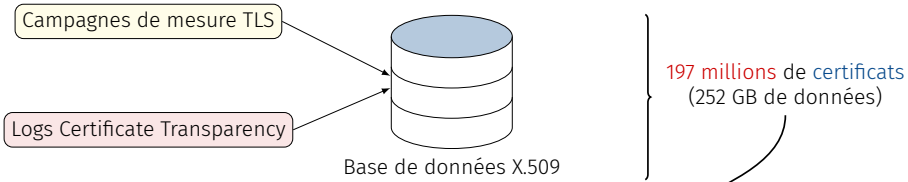
Intérêts

Décisions d'implémentation

Validations

Data set

Origine et contenu

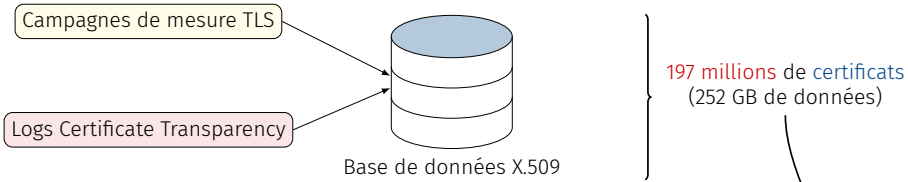


Intérêts

- Décisions d'implémentation
- Validations
- Non régression

DATA SET

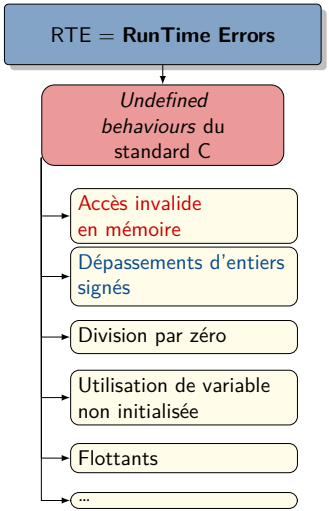
Origine et contenu



Intérêts

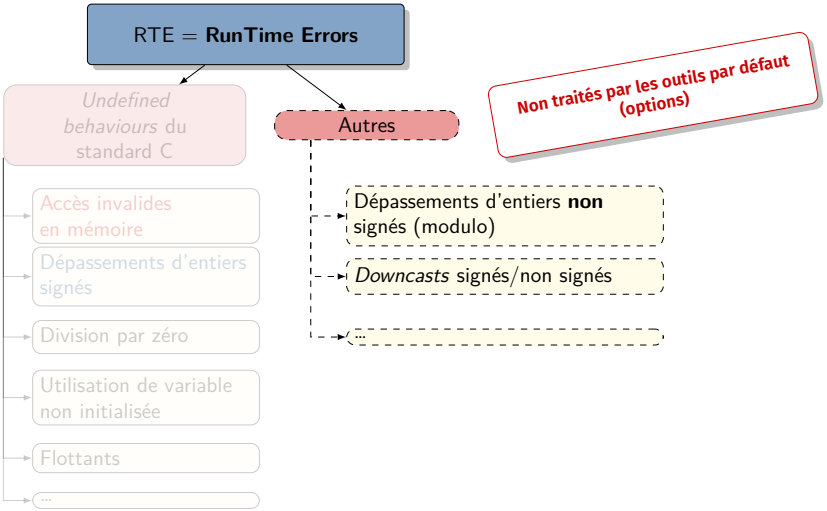
- Décisions d'implémentation
- Validations
- Non régression
- Optimisation/performances (200.000 certificats/seconde)

Absence complète de RTE ?

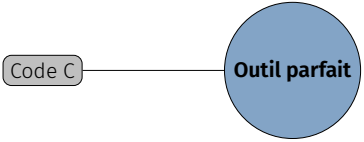


Classiquement traités par les outils

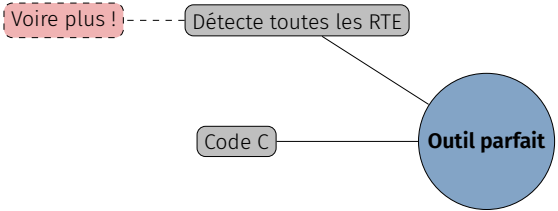
Absence complète de RTE ?



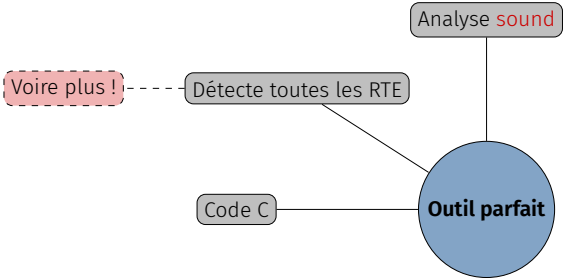
Choix des armes



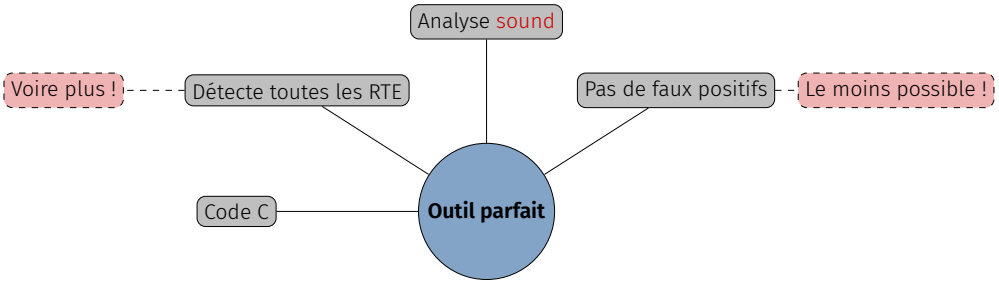
Choix des armes



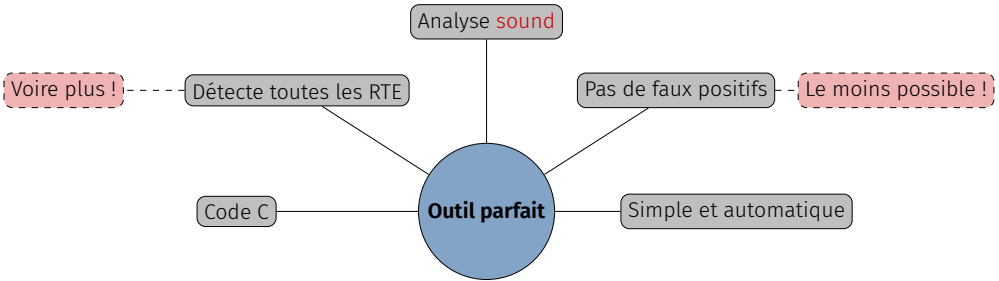
Choix des armes



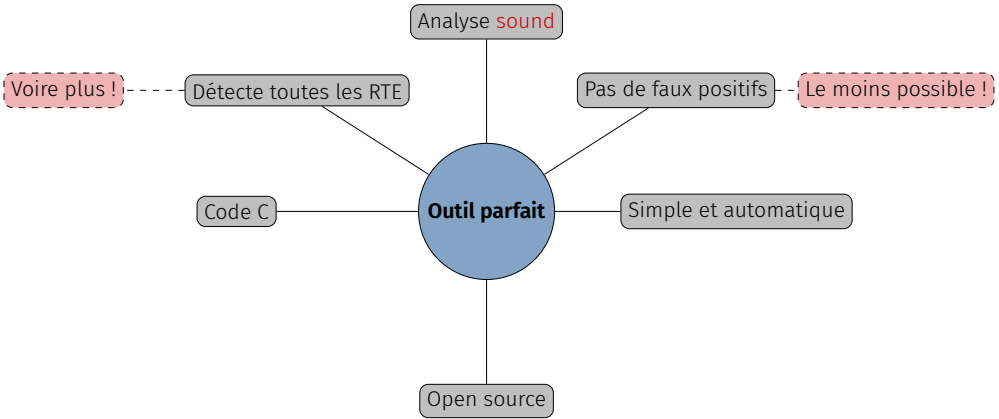
Choix des armes



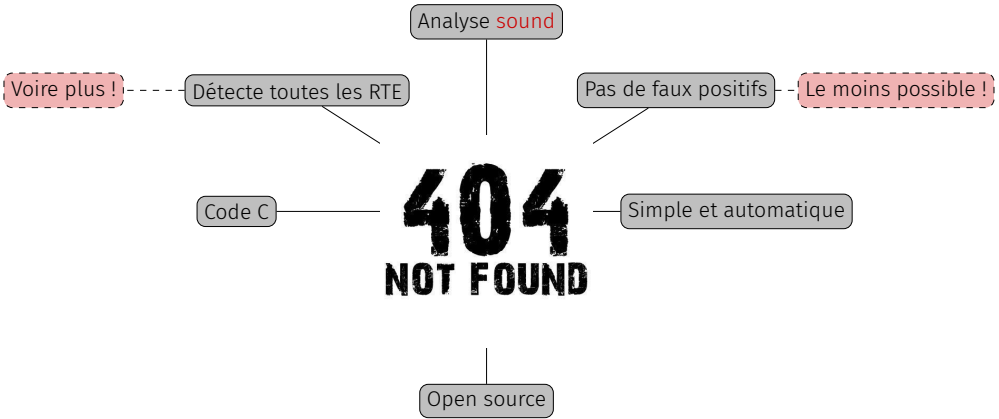
Choix des armes



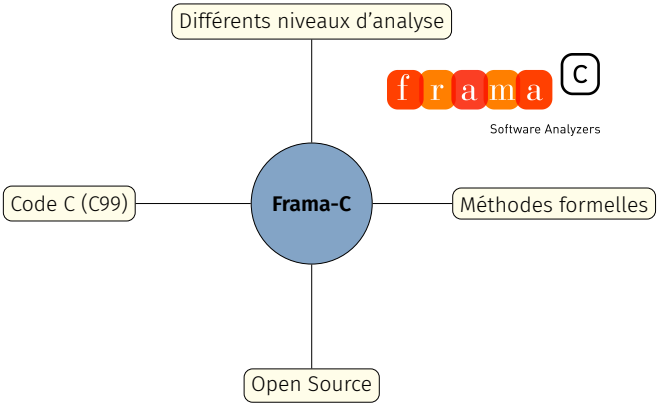
Choix des armes



Choix des armes



Frama-C

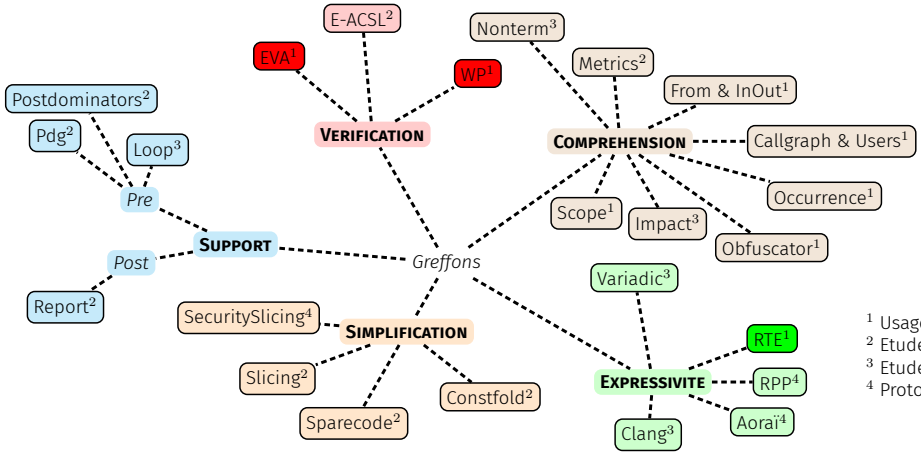

Différents niveaux d'analyse
frama C
Software Analyzers
Code C (C99)
Frama-C
Méthodes formelles
Open Source

Frama-C, plus concrètement

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

Frama-C, plus concrètement

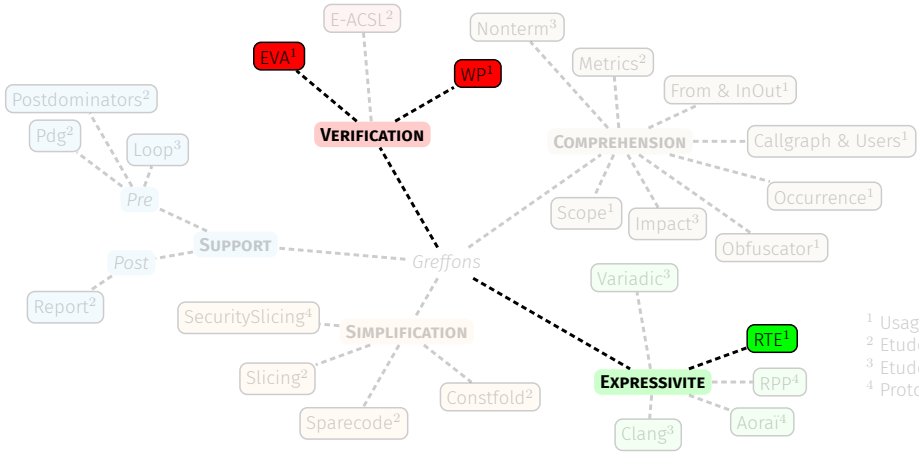
Un schéma vaut mieux qu'un long discours ...



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

Frama-C, plus concrètement

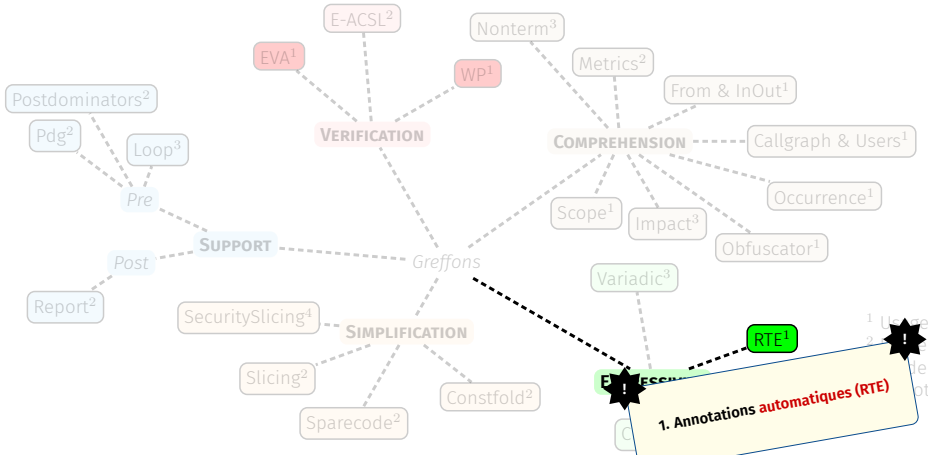
Un schéma vaut mieux qu'un long discours ...



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

Frama-C, plus concrètement

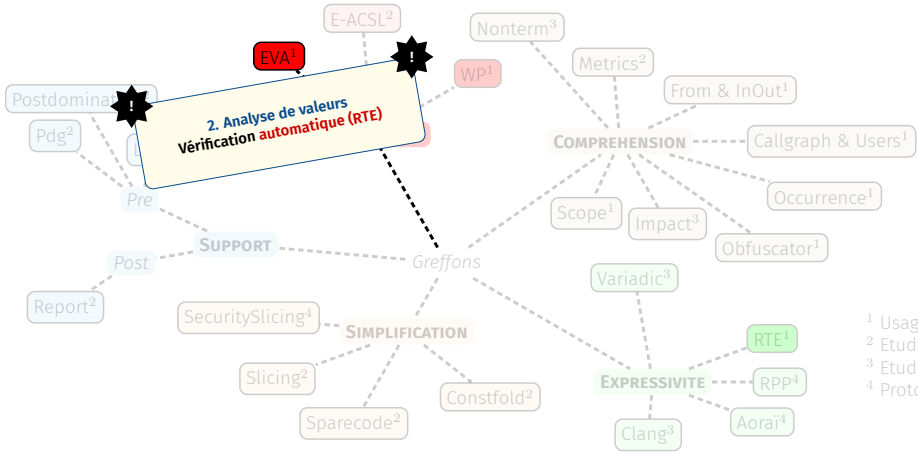
Un schéma vaut mieux qu'un long discours ...



[1] Usage industriel
[2] Étude de cas industriel
[3] Étude de cas interne CEA
[4] Prototype

FRAMA-C, PLUS CONCRÈTEMENT

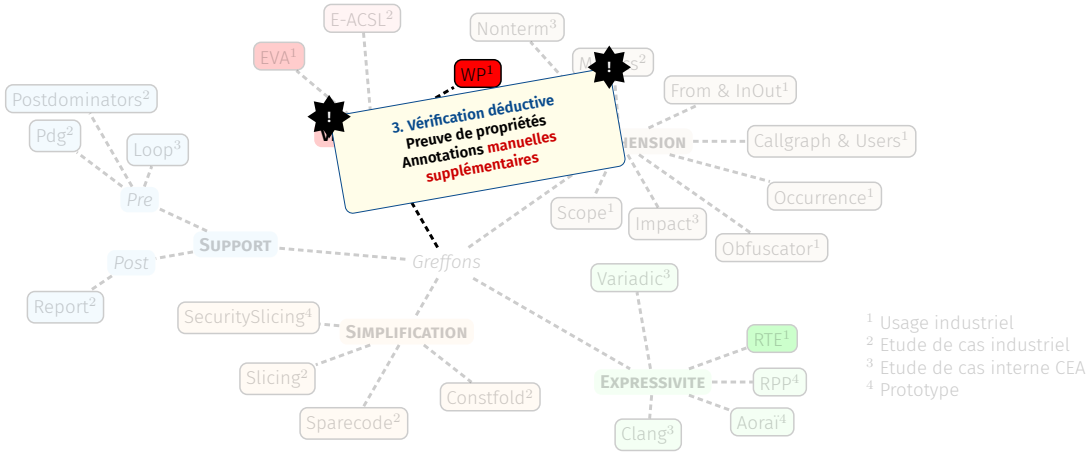
Un schéma vaut mieux qu'un long discours ...



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

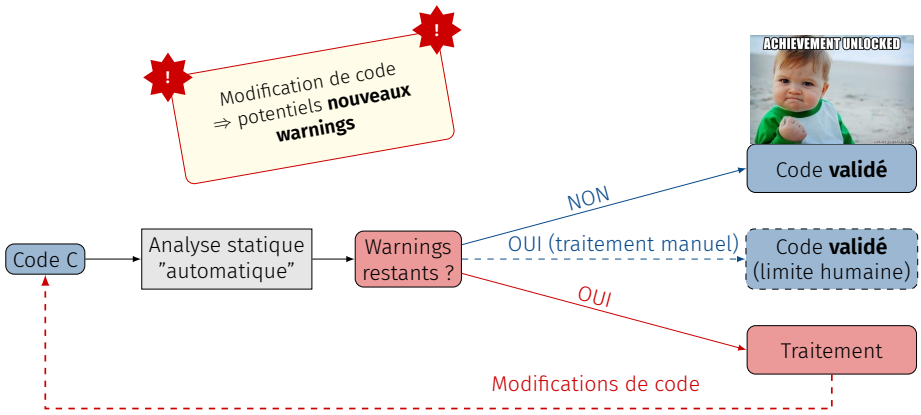
Frama-C, plus concrètement

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



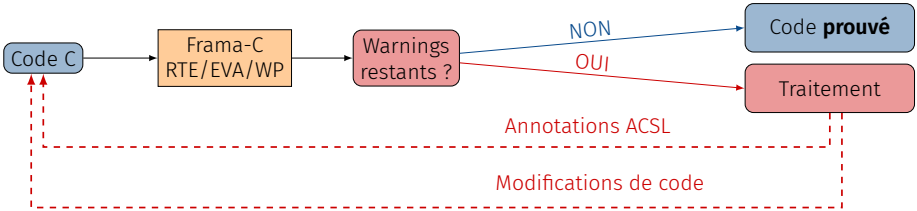
[1] Usage industriel
[2] Etude de cas industriel
[3] Etude de cas interne CEA
[4] Prototype

Workflow d'ANALYSE STATIQUE CLASSIQUE



Workflow avec stratégie EVA/WP

Base de code prouvée
⇒ **facilité** d'évolution



ACSL

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)
{
    /*...*/

}
```

ACSL

Deuxième exemple : une boucle

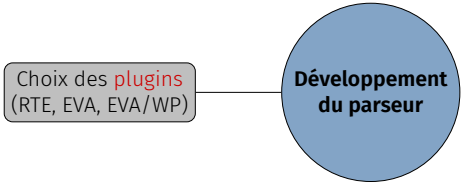
```
static int check_printable_string(const u8 *buf, u16 len)
{
    /*@ loop invariant 0 <= rbytes <= len;
      @ loop assigns rbytes, c, ret;
      @ loop variant (len - rbytes);
      @ */
    for (rbytes = 0; rbytes < len; rbytes++) {
        c = buf[rbytes];
        if ((c >= 'a' && c <= 'z') ||
            (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

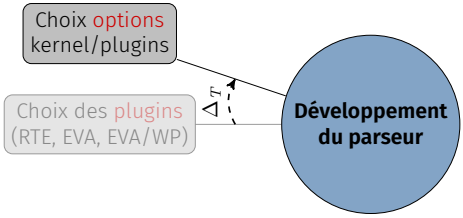
Au final

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

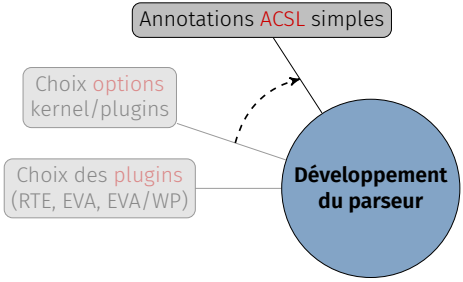
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



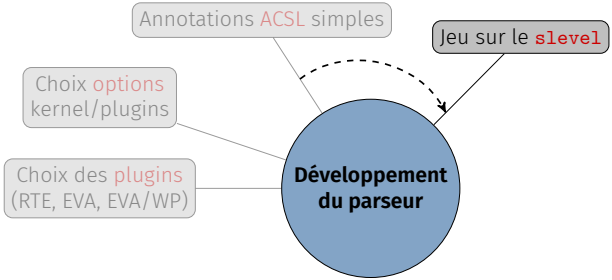
Retex Frama-C : mise en oeuvre dans le projet



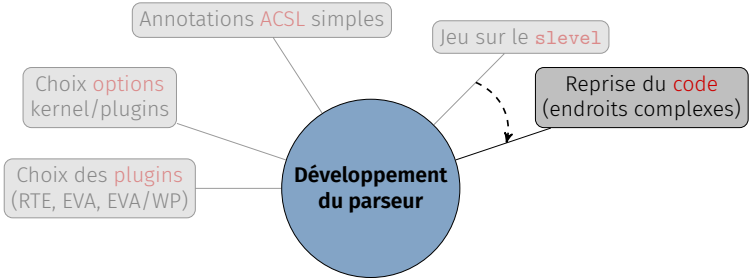
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



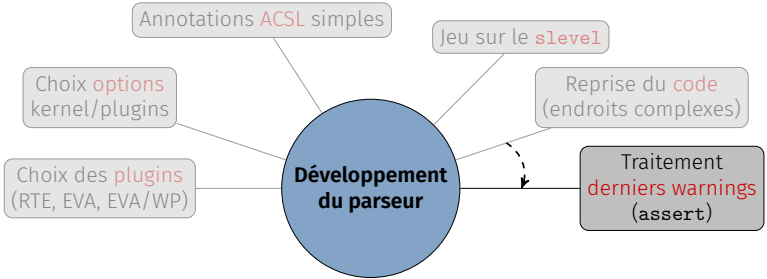
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



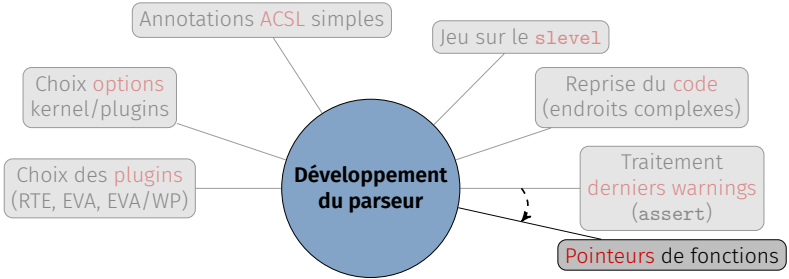
Retex Frama-C : mise en oeuvre dans le projet



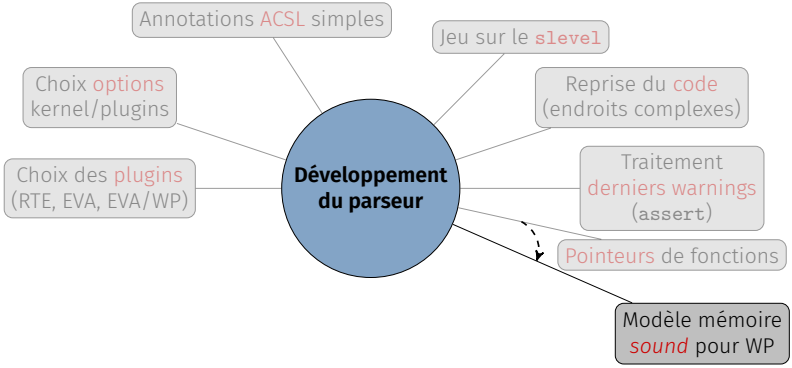
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



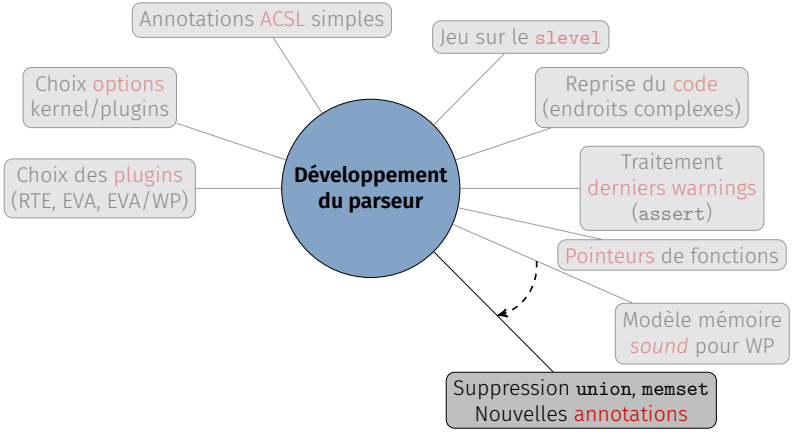
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



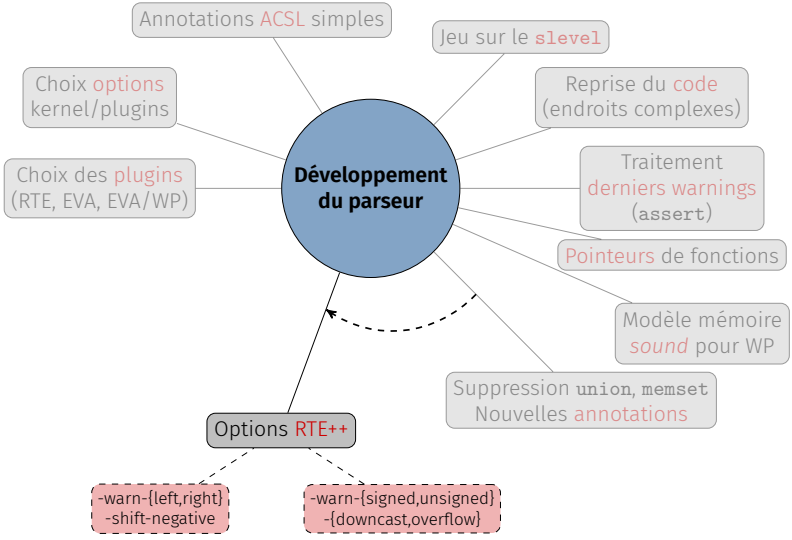
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



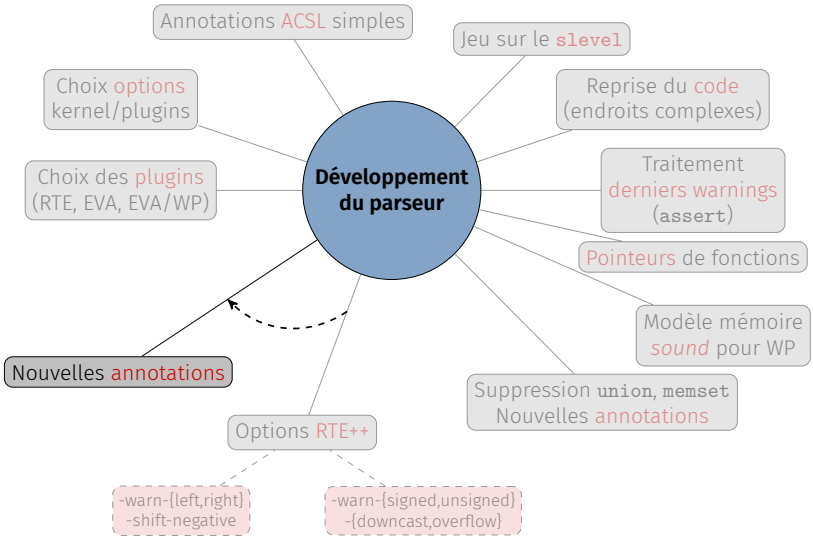
RETEX FRAMA-C : MISE EN OEUVRE DANS LE PROJET



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

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

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_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) {
        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_algoid_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_algoid_params = parse_algoid_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]))
```

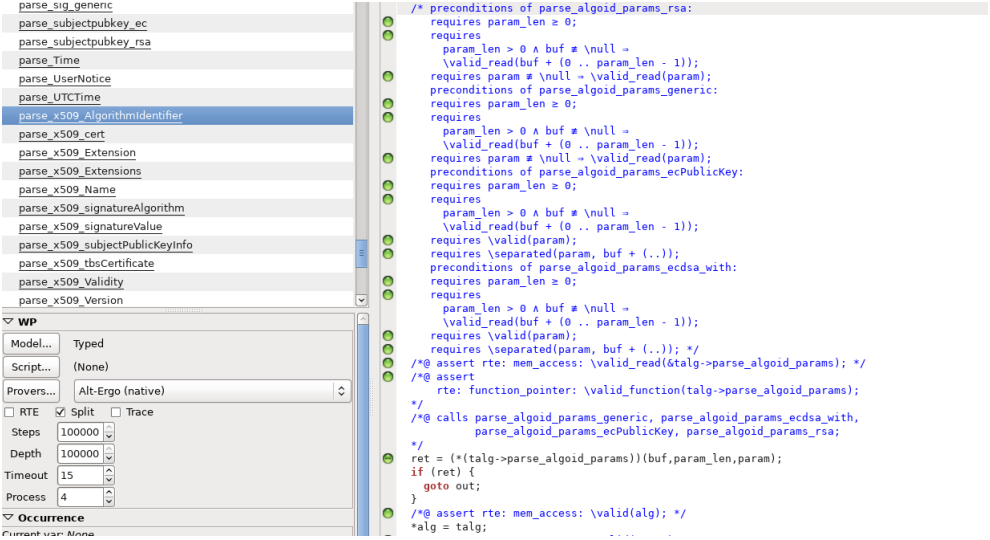
RETEX FRAMA-C : POINTEURS DE FONCTION

```
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_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) {
        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;
}
```

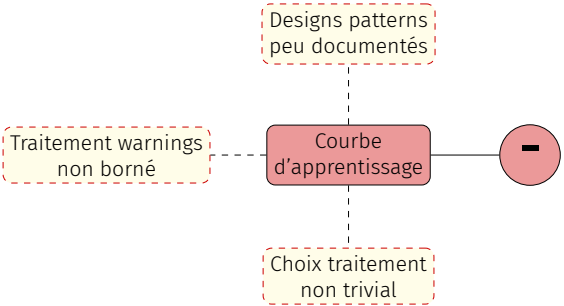
```
typedef struct {
    const u8 *alg_name;
    const u8 *alg_printable_oid;
    const u8 *alg_der_oid;
    const u8 alg_der_oid_len;
    const u8 alg_type;
    int (*parse_sig)(const u8 *buf, u16 len, u16 *eaten);
    int (*parse_subjectpubkey)(const u8 *buf, u16 len, alg_param *param);
    int (*parse_algoid_params)(const 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_algoid_params = parse_algoid_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

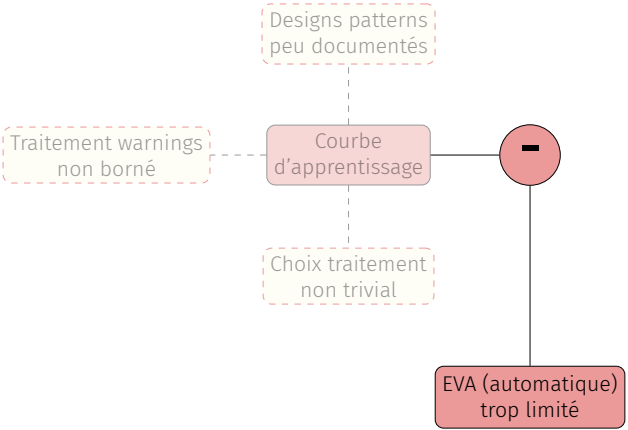


Retex Frama-C : l'outil

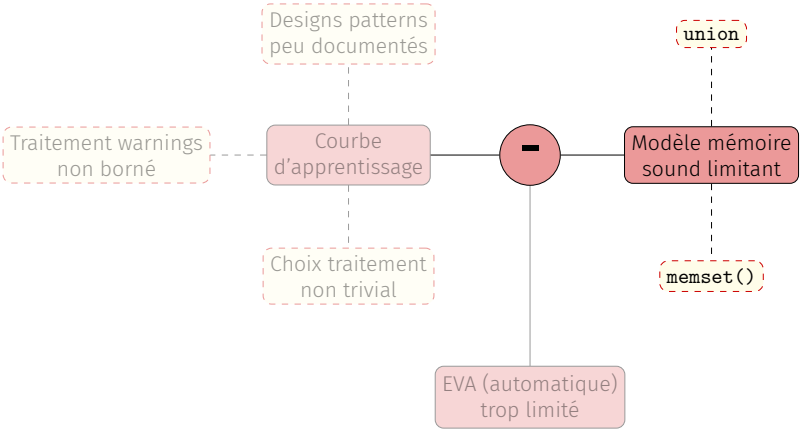
RETEX FRAMA-C : L'OUTIL



RETEX FRAMA-C : L'OUTIL

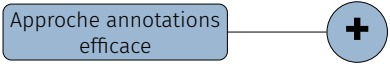


RETEX FRAMA-C : L'OUTIL

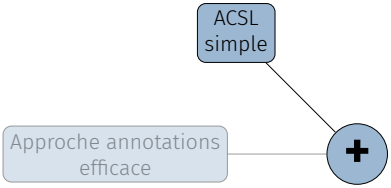


RETEX FRAMA-C : L'OUTIL

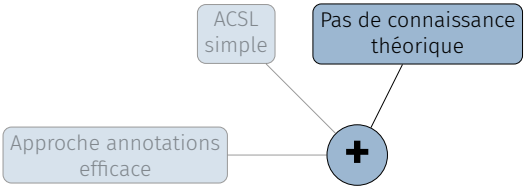
RETEX FRAMA-C : L'OUTIL



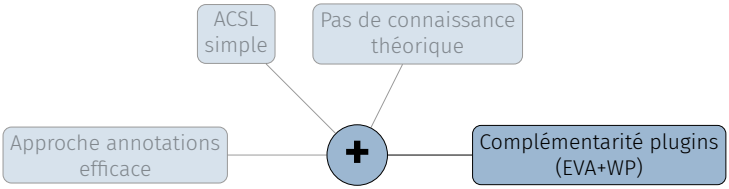
RETEX FRAMA-C : L'OUTIL



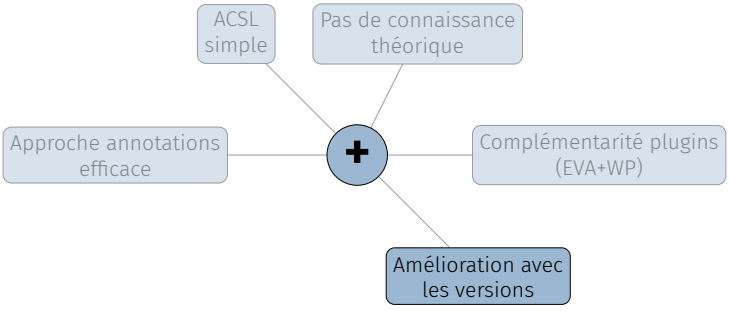
RETEX FRAMA-C : L'OUTIL



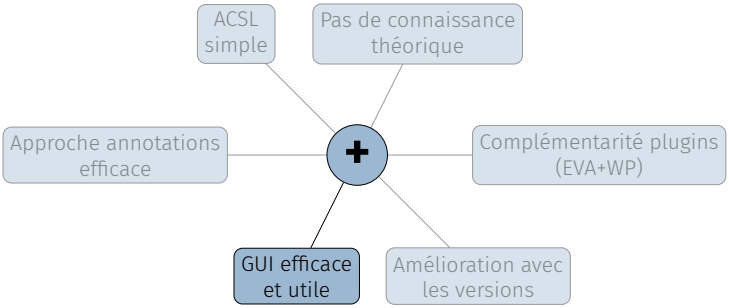
RETEX FRAMA-C : L'OUTIL



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

Fausses 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

Fausses 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, ...


WHO?WHERE?WHAT?
WHEN?WHY?HOW?
HOW?WHAT?WHO?
WHO?WHERE?WHERE?
WHAT?WHY?WHAT?
WHERE?WHEN?
WHERE?WHO?
HOW?WHAT?
WHO?WHERE?
WHY?WHAT?
WHO?WHEN?
WHO?WHY?HOW?
HOW?WHERE?
WHEN?WHY?
WHO?WHAT?
WHAT?HOW?
WHAT?WHEN?

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