



Mind your Language(s)!

Langages de développement et sécurité

É. JAEGER, Ministère de la Défense
(P. CHIFFLIER & O. LEVILLAIN, ANSSI)

An unreliable programming language generating unreliable programs constitutes a far greater risk to our environment and to our society than unsafe cars, toxic pesticides, or accidents at nuclear power stations. Be vigilant to reduce that risk, not to increase it.

C.A.R. Hoare

les Himba de Namibie consacrent une catégorie entière aux bleu et vert vifs : parmi des figures vert vif, ils savent identifier un vert légèrement différent pour lequel ils disposent d'un mot distinct. Mais au milieu de figures vertes, parmi lesquelles on en aura glissé une bleue choisie pour avoir le même nom que le vert, les Himba repéreront difficilement l'intrus. . .

Science & Vie, 2014

The tools we are trying to use and the language or notations we are using to express or record our thoughts, are the major factor determining what we can think or express at all !

Edsger W. Dijkstra

Don't you see that the whole aim of Newspeak is to narrow the range of thought ? In the end we shall make thought-crime literally impossible, because there will be no words in which to express it.

1984, George Orwell



Spécification de deux fonctions pour la compression (Zip) et la décompression (Unzip) de fichiers

Fonctionnel

- ▶ $\forall (f : \text{File}), \text{Unzip}(\text{Zip } f) = f$

Sécurité

- ▶ $\forall (c : \text{File}), (\neg \exists (f : \text{File}), \text{Zip } f = c) \Rightarrow \text{Unzip } c = \text{Error}$
- ▶ En particulier, ne pas faire confiance à un champ annonçant à l'avance la taille du fichier décompressé



Quelques aspects intéressants d'un langage en termes de sécurité

- ▶ Faux amis ou pièges
- ▶ Constructions non spécifiées ou non définies mais disponibles
- ▶ Possibilités d'offuscation pour un développeur malicieux
- ▶ Bugs ou comportements inappropriés des outils de développement
- ▶ Limitations des capacités d'analyse
- ▶ Surprises à l'exécution
- ▶ ...

Ce qui est signalé dans la suite n'est pas forcément une erreur, mais « attire l'attention » des experts en sécurité

Réciproquement, les problèmes non liés aux langages (algorithmes, architectures, *etc.*) sont hors sujet ici



Plan

- 1 Toi qui entres ici. . .
- 2 Au-delà des illustrations
- 3 Quelques éléments de conclusion



- 1 **Toi qui entres ici...**
 - Lutte des classes
 - Mise en boîte
 - Effets spéciaux
 - Épreuves d'adresses
 - *Cast-o-rama*
 - Rencontre du 3^e type
 - Où tout est question d'interprétation
 - Les liaisons dangereuses
 - Syntaxe, priez pour nous



Le comportement des programmes objet très simples est parfois surprenant : que fait le code suivant lorsque `Mathf.pi=3.1415` ?

Source (java/StaticInit.java)

```
class StaticInit {
    public static void main(String[] args) {
        if (Mathf.pi-3.1415<0.0001)
            System.out.println("Hello world");
        else
            System.out.println("Hello strange universe");
    }
}
```



Le comportement des programmes objet très simples est parfois surprenant : que fait le code suivant lorsque `Mathf.pi=3.1415` ?

Source (java/StaticInit.java)

```
class StaticInit {
    public static void main(String[] args) {
        if (Mathf.pi-3.1415<0.0001)
            System.out.println("Hello world");
        else
            System.out.println("Hello strange universe");
    }
}
```

À l'exécution, on obtient `Bad things happen!`



L'explication du comportement de `StaticInit` se trouve dans `Mathf`

Source (java/Mathf.java)

```
class Mathf {
    static double pi=3.1415;
    static { // Do whatever you want here
        System.out.println("Bad things happen!");
        // Do not return to calling class
        System.exit(0); }
}
```

En JAVA le chargement d'une classe exécute le code d'initialisation de classe, même en l'absence d'appel à une méthode ou à un constructeur



Évitons donc toute référence à une classe externe non maîtrisée

Source (java/Deserial.java)

```
import java.io.*;
class Friend { } // Unlikely to be dangerous!
class Deserial {
    public static void main (String[] args)
        throws FileNotFoundException, IOException,
            ClassNotFoundException {
        FileInputStream fis = new FileInputStream("friend");
        ObjectInputStream ois = new ObjectInputStream(fis);
        Friend f=(Friend)ois.readObject();
        System.out.println("Hello world");
    }
}
```



Évitons donc toute référence à une classe externe non maîtrisée

Source (java/Deserial.java)

```
import java.io.*;
class Friend { } // Unlikely to be dangerous!
class Deserial {
    public static void main (String[] args)
        throws FileNotFoundException, IOException,
            ClassNotFoundException {
        FileInputStream fis = new FileInputStream("friend");
        ObjectInputStream ois = new ObjectInputStream(fis);
        Friend f=(Friend)ois.readObject();
        System.out.println("Hello world");
    }
}
```

Hélas à l'exécution on a **Bad things happen!** Le fichier sérialisé contient la classe de l'objet, lorsque le *cast* échoue c'est déjà trop tard



1 Toi qui entres ici...

- Lutte des classes
- **Mise en boîte**
- Effets spéciaux
- Épreuves d'adresses
- *Cast-o-rama*
- Rencontre du 3^e type
- Où tout est question d'interprétation
- Les liaisons dangereuses
- Syntaxe, priez pour nous



En guide d'introduction, un petit rappel...

Source (java/PrivArrayAccess.java)

```
class PrivArray {
    static private int[] tab={1,2};
    static public int[] get() { return tab; } // No set!
    static public void print()
        { System.out.println(tab[0]+", "+tab[1]); }
}

class PrivArrayAccess {
    public static void main (String[] args) {
        PrivArray.print();
        PrivArray.get()[1]=3; // Do you set?
        PrivArray.print();
    }
}
```

Le programme affiche 1,2 puis 1,3...



[JAVA] Encore une objection

L'encapsulation objet est-elle un mécanisme de sécurité ?

Source (java/Introspect.java)

```
import java.lang.reflect.*;
class Secret { private int x = 42; }
public class Introspect {
    public static void main (String[] args) {
        try { Secret o = new Secret();
            Class c = o.getClass();
            Field f = c.getDeclaredField("x");
            f.setAccessible(true);
            System.out.println("x="+f.getInt(o));
        }
        catch (Exception e) { System.out.println(e); }
    }
}
```

L'introspection peut être interdite dans la politique de sécurité JAVA, mais c'est complexe et des effets secondaires sont probables



OCAML offre également différents mécanismes d'encapsulation ¹

Source (ocaml/hsm.ml)

```
module type Crypto = sig val id:int end;;

module C : Crypto =
struct
  let id=Random.self_init(); Random.int 8192
  let key=Random.self_init(); Random.int 8192
end;;
```

C'est un boîte fermée ; la valeur `id` est visible et celle de `key` masquée

`C.id` donne - : int = 2570

`C.key` donne `Error: Unbound value C.key`

1. Ici les modules, sachant que les objets d'OCAML sont plus « fragiles »



Mais cette encapsulation peut être contournée

Source (ocaml/hsmoracle.ml)

```
let rec oracle o1 o2 =
  let o = (o1 + o2)/2 in
  let module O = struct let id=C.id let key=o end in
  if (module O:Crypt0)>(module C:Crypt0)
  then oracle o1 o
  else (if (module O:Crypt0)<(module C:Crypt0)
        then oracle o o2
        else o);;

oracle 0 8192;;
```

À l'exécution, la valeur de `key` est retournée ; impossible d'ouvrir la boîte, mais on peut la comparer à d'autres sur une balance



Pas convaincu ? Remettons en cause le typage, alors...

Source (ocaml/hsm5.ml)

```
module type Crypto = sig val id:int end;;

module C : Crypto =
struct
  let id=42
  let secretchar='k'
end;;

let rec oracle o1 o2 =
  let o = (o1 + o2)/2 in
  let module O = struct let id=C.id let key=o end in
  if (module O:Crypto)>(module C:Crypto)
  then oracle o1 o
  else (if (module O:Crypto)<(module C:Crypto)
        then oracle o o2 else o);;
```

L'oracle retourne 107, le code ASCII du caractère 'k'



JAVA permet de définir des classes internes

Source (java/Innerclass.java)

```
public class Innerclass {
    private static int a=42;

    static public class Innerinner {
        private static int b=54;
        public static void print() {
            System.out.println(Innerclass.a);
        }
    }

    public static void main (String[] args) {
        System.out.println(Innerinner.b);
        Innerinner.print();
    }
}
```

Pourtant les classes internes ne sont pas supportées en *bytecode*!



- 1 **Toi qui entres ici...**
 - Lutte des classes
 - Mise en boîte
 - **Effets spéciaux**
 - Épreuves d'adresses
 - *Cast-o-rama*
 - Rencontre du 3^e type
 - Où tout est question d'interprétation
 - Les liaisons dangereuses
 - Syntaxe, priez pour nous



[C] Questions stratégiques

Si on joue avec les effets de bord, la stratégie d'évaluation devient significative, et des subtilités peuvent apparaître

Source (c/effect.c)

```
{ int c=0; printf("%d %d\n",c++,c++); }
```

```
{ int c=0; printf("%d %d\n",++c,++c); }
```

```
{ int c=0; printf("%d %d\n",c=1,c=2); }
```



[C] Questions stratégiques

Si on joue avec les effets de bord, la stratégie d'évaluation devient significative, et des subtilités peuvent apparaître

Source (c/effect.c)

```
{ int c=0; printf("%d %d\n",c++,c++); }  
{ int c=0; printf("%d %d\n",++c,++c); }  
{ int c=0; printf("%d %d\n",c=1,c=2); }
```

La première ligne affiche 1 0



[C] Questions stratégiques

Si on joue avec les effets de bord, la stratégie d'évaluation devient significative, et des subtilités peuvent apparaître

Source (c/effect.c)

```
{ int c=0; printf("%d %d\n",c++,c++); }  
{ int c=0; printf("%d %d\n",++c,++c); }  
{ int c=0; printf("%d %d\n",c=1,c=2); }
```

La première ligne affiche 1 0

La seconde ligne affiche 2 2



[C] Questions stratégiques

Si on joue avec les effets de bord, la stratégie d'évaluation devient significative, et des subtilités peuvent apparaître

Source (c/effect.c)

```
{ int c=0; printf("%d %d\n",c++,c++); }  
{ int c=0; printf("%d %d\n",++c,++c); }  
{ int c=0; printf("%d %d\n",c=1,c=2); }
```

La première ligne affiche 1 0

La seconde ligne affiche 2 2

La troisième ligne affiche 1 1



En OCAML le code est statique et les chaînes sont mutables ; mais qu'en est-il des chaînes apparaissant dans le code ?

Source (ocaml/mutable.ml)

```
let check c =  
  if c then "OK" else "KO";;  
  
let f=check false in  
  f.[0]<- '0'; f.[1]<- 'K';;  
  
check true;;  
check false;;
```



En OCAML le code est statique et les chaînes sont mutables ; mais qu'en est-il des chaînes apparaissant dans le code ?

Source (ocaml/mutable.ml)

```
let check c =  
  if c then "OK" else "KO";;  
  
let f=check false in  
  f.[0]<- '0'; f.[1]<- 'K';;  
  
check true;;  
check false;;
```

Les deux applications de `check` renvoient "OK"



L'exemple précédent n'est pas une redéfinition de la fonction `alert` mais un simple effet de bord ; pour s'en convaincre, voici ce que cela donne avec une fonction de la bibliothèque standard

Source (ocaml/mutablebool.ml)

```
let t=string_of_bool true in
    t.[0]<- 'f'; t.[1]<- 'a'; t.[3]<- 'x';;

Printf.printf "1=1 est %b\n" (1=1);;
```

Le code affiche `1=1 est faux` ; d'autres fonctions intéressantes sont concernées, par exemple `Char.escaped (!)` ainsi que certains *patterns* de développement usuels basés sur les exceptions



Au préalable, deux petits rappels

Source (c/strategy1.c)

```
#define abs(X) (X)>=0?(X):(-X)
int abs(int x) { return x>=0?x:-x; }

#define first(x,y) x
int first(int x,int y) { return x; }
```



Au préalable, deux petits rappels

Source (c/strategy1.c)

```
#define abs(X) (X)>=0?(X):(-X)
int abs(int x) { return x>=0?x:-x; }

#define first(x,y) x
int first(int x,int y) { return x; }
```

Les deux versions de `abs` n'ont pas le même comportement par exemple pour `abs(x++)`



Au préalable, deux petits rappels

Source (c/strategy1.c)

```
#define abs(X) (X)>=0?(X):(-X)
int abs(int x) { return x>=0?x:-x; }

#define first(x,y) x
int first(int x,int y) { return x; }
```

Les deux versions de `abs` n'ont pas le même comportement par exemple pour `abs(x++)`

Les deux versions de `first` n'ont pas le même comportement par exemple pour `first(x,1/x)` avec `x` valant `0` – les exceptions sont des effets de bord



Ces subtilités étant clarifiées, que font les deux codes suivants ?

Source (c/strategy3.c)

```
int zero(int x) { return 0; }  
int main(void) { int x=0; x=zero(1/x); return 0; }
```

Source (c/strategy3b.c)

```
int zero(int x) { return 0; }  
int main(void) { int x=0; return zero(1/x); }
```



Ces subtilités étant clarifiées, que font les deux codes suivants ?

Source (c/strategy3.c)

```
int zero(int x) { return 0; }
int main(void) { int x=0; x=zero(1/x); return 0; }
```

Source (c/strategy3b.c)

```
int zero(int x) { return 0; }
int main(void) { int x=0; return zero(1/x); }
```

Tout dépend du niveau d'optimisation

- ▶ -O0 : Floating point exception (core dumped)
- ▶ -O1 : le premier programme termine normalement
- ▶ -O2 : les deux programmes terminent normalement



Plan

1 Toi qui entres ici...

- Lutte des classes
- Mise en boîte
- Effets spéciaux
- **Épreuves d'adresses**
- *Cast-o-rama*
- Rencontre du 3^e type
- Où tout est question d'interprétation
- Les liaisons dangereuses
- Syntaxe, priez pour nous



Petit rappel sur le principe des *Buffer Overflows*²

Source (c/overflow.c)

```
#include <stdio.h>
#include <stdlib.h>

void set(int s,int v) { *(&s-s)=v; }

void bad() { printf("Bad things happen!\n"); exit(0); }

int main(void) {
    set(1,(int)bad); printf("Hello world\n"); return 0;
}
```

2. Ici dans une version balèze, car sans *Buffer*



Petit rappel sur le principe des *Buffer Overflows*²

Source (c/overflow.c)

```
#include <stdio.h>
#include <stdlib.h>

void set(int s,int v) { *(&s-s)=v; }

void bad() { printf("Bad things happen!\n"); exit(0); }

int main(void) {
    set(1,(int)bad); printf("Hello world\n"); return 0;
}
```

Bad things happen! La pile est corrompue, on peut surcharger des variables, modifier une adresse de retour voire injecter du code...

2. Ici dans une version balèze, car sans *Buffer*



[C] Faire mauvaise impression

Mais les manipulations de piles sont parfois bien cachées...

Source (c/stringformat3.c)

```
#include <stdio.h>

char *f="%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.\
%08x.%08x.%08x.%08x.%08x.%08x.%n";

void strfmtattack() { printf(f); }

int main(void) {
    int s=0x12345;
    int *p=&s;
    strfmtattack();
    if (s!=0x12345) printf("Bad things happen! s=%08x\n",s);
    return 0;
}
```



[C] Faire mauvaise impression

Mais les manipulations de piles sont parfois bien cachées...

Source (c/stringformat3.c)

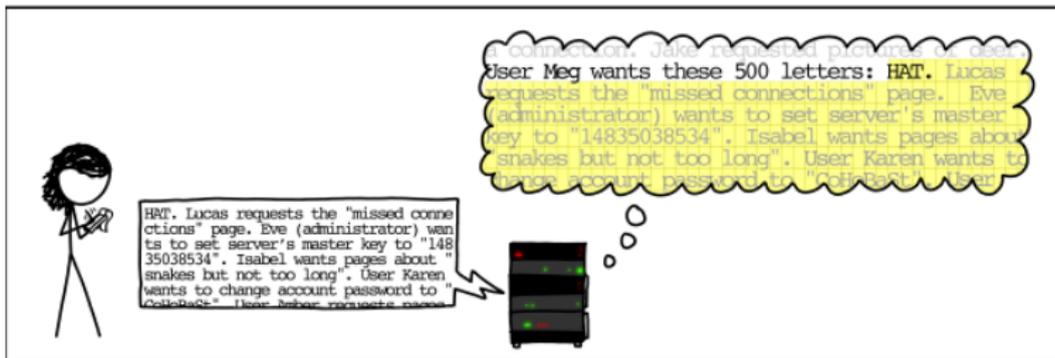
```
#include <stdio.h>

char *f="%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.\
%08x.%08x.%08x.%08x.%08x.%08x.%n";

void strfmtattack() { printf(f); }

int main(void) {
    int s=0x12345;
    int *p=&s;
    strfmtattack();
    if (s!=0x12345) printf("Bad things happen! s=%08x\n",s);
    return 0;
}
```

...0036b225.00fdd280.00000000.00012345.Bad things happen! s=0000007e





La faille *Heartbleed* (CVE-2014-160) a été révélée en avril 2014

Concrètement, un serveur HTTPS sur deux de la planète était concerné avec une compromission possible

- ▶ des clés privées
- ▶ des mots de passe
- ▶ de toute autre information présente en mémoire du process...

L'intégration de ce service de sécurité cryptographique a induit une vulnérabilité dont l'impact va très au-delà du périmètre de ce service

C'est un simple oubli de vérification de bornes dans le code d'une fonction non critique du protocole SSL/TLS



La faille *Heartbleed* (CVE-2014-160) a été révélée en avril 2014

Concrètement, un serveur HTTPS sur deux de la planète était concerné avec une compromission possible

- ▶ des clés privées
- ▶ des mots de passe
- ▶ de toute autre information présente en mémoire du process...

L'intégration de ce service de sécurité cryptographique a induit une vulnérabilité dont l'impact va très au-delà du périmètre de ce service

C'est un simple oubli de vérification de bornes dans le code d'une fonction non critique du protocole SSL/TLS

Il est temps de se rappeler où l'on trouve des serveur HTTPS...



- 1 Toi qui entres ici...
 - Lutte des classes
 - Mise en boîte
 - Effets spéciaux
 - Épreuves d'adresses
 - **Cast-o-rama**
 - Rencontre du 3^e type
 - Où tout est question d'interprétation
 - Les liaisons dangereuses
 - Syntaxe, priez pour nous



[ERLANG] Let it crash (indeed)

ERLANG propose surcharges et conversions automatiques (*cast*) : $1+1$, $1.0+1.0$ et $1+1.0$ sont des expressions valides³

Source (erlang/factorial.erl)

```
-module(factorial).  
-compile(export_all).  
  
fact(0) -> 1;  
fact(N) -> N*fact(N-1).
```

3. Et il serait inutile de s'embêter à distinguer entiers et flottants...



[ERLANG] Let it crash (indeed)

ERLANG propose surcharges et conversions automatiques (*cast*) : $1+1$, $1.0+1.0$ et $1+1.0$ sont des expressions valides³

Source (erlang/factorial.erl)

```
-module(factorial).  
-compile(export_all).  
  
fact(0) -> 1;  
fact(N) -> N*fact(N-1).
```

```
demo$ erl
```

```
1> factorial:fact(4).
```

```
24
```

```
2> factorial:fact(4.0).
```

```
heap_alloc: Cannot allocate...
```

3. Et il serait inutile de s'embêter à distinguer entiers et flottants...



[JAVASCRIPT] Certains sont plus égaux que d'autres

JAVASCRIPT offre également tout le confort moderne...

Source (js/unification2.js)

```
if (0=='0') print("Equal"); else print("Different");

switch (0)
{ case '0':print("Equal");
  default:print("Different");
}
```



[JAVASCRIPT] Certains sont plus égaux que d'autres

JAVASCRIPT offre également tout le confort moderne...

Source (js/unification2.js)

```
if (0=='0') print("Equal"); else print("Different");

switch (0)
{ case '0':print("Equal");
  default:print("Different");
}
```

L'affichage obtenu est `Equal` puis `Different`



[JAVA] Encore une égalité contrariante

Au moins avec l'égalité physique, on sait à quoi s'en tenir... sauf en cas d'interactions subtiles avec des bibliothèques standards innovantes

Source (java/IntegerBoxing.java)

```
Integer a1=42;
Integer a2=42;
if (a1==a2) System.out.println("a1 == a2");

Integer b1=1000;
Integer b2=1000;
if (b1==b2) System.out.println("b1 == b2");
```



[JAVA] Encore une égalité contrariante

Au moins avec l'égalité physique, on sait à quoi s'en tenir... sauf en cas d'interactions subtiles avec des bibliothèques standards innovantes

Source (java/IntegerBoxing.java)

```
Integer a1=42;
Integer a2=42;
if (a1==a2) System.out.println("a1 == a2");

Integer b1=1000;
Integer b2=1000;
if (b1==b2) System.out.println("b1 == b2");
```

`a1==a2`, mais pas de second affichage, qui veut jouer aux devinettes ?



Faut-il préférer *cast* et surcharge, ou associativité et transitivité ?



Faut-il préférer *cast* et surcharge, ou associativité et transitivité ?

En JAVASCRIPT, on a `'0'==0` qui est vrai, de même `0=='0.0'`, par contre `'0'=='0.0'` est faux ; en d'autres termes, l'égalité n'est pas transitive



Faut-il préférer *cast* et surcharge, ou associativité et transitivité ?

En JAVASCRIPT, on a `'0'==0` qui est vrai, de même `0=='0.0'`, par contre `'0'=='0.0'` est faux ; en d'autres termes, l'égalité n'est pas transitive

Autre exemple avec l'opérateur `+`, qui peut être l'addition d'entiers ou la concaténation de chaînes, mais qui est dans les deux cas associatif

Source (js/cast3.js)

```
a=1; b=2; c='Foo';  
print(a+b+c); print(c+a+b); print(c+(a+b));
```



Faut-il préférer *cast* et surcharge, ou associativité et transitivité ?

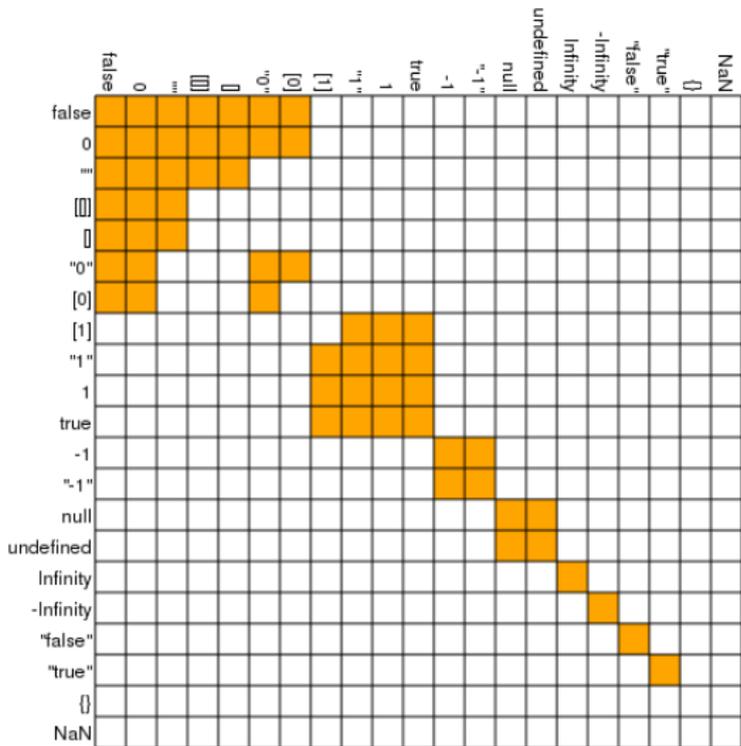
En JAVASCRIPT, on a `'0'==0` qui est vrai, de même `0=='0.0'`, par contre `'0'=='0.0'` est faux ; en d'autres termes, l'égalité n'est pas transitive

Autre exemple avec l'opérateur `+`, qui peut être l'addition d'entiers ou la concaténation de chaînes, mais qui est dans les deux cas associatif

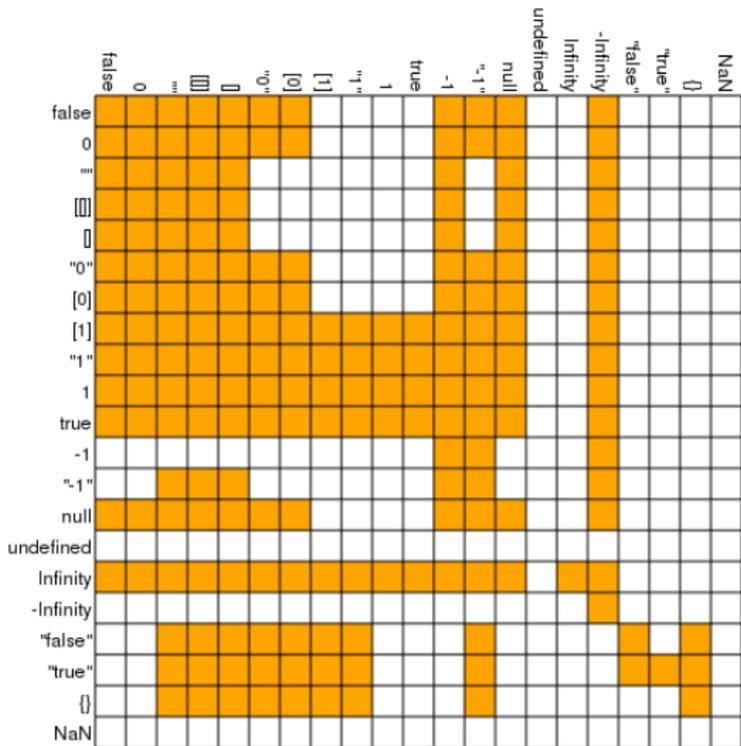
Source (js/cast3.js)

```
a=1; b=2; c='Foo';  
print(a+b+c); print(c+a+b); print(c+(a+b));
```

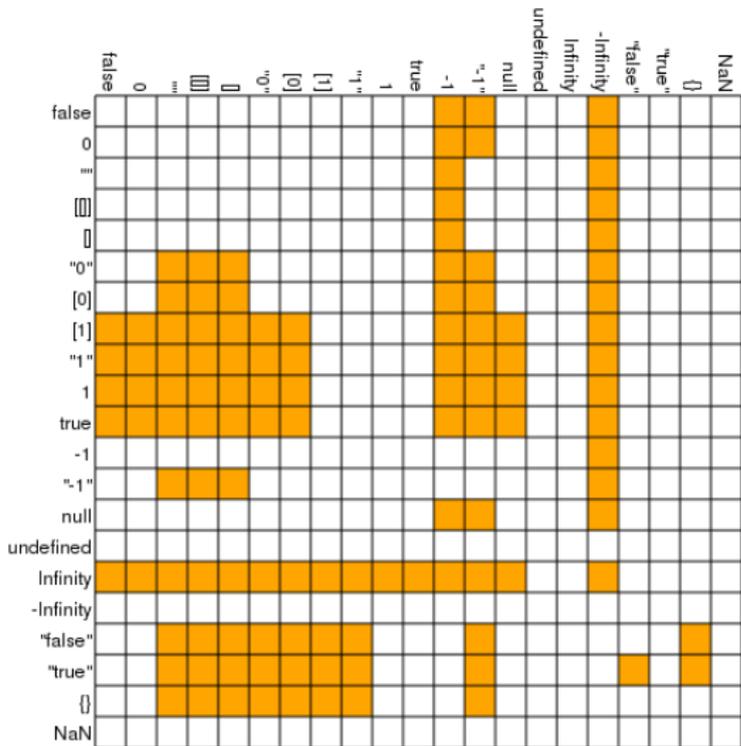
`3Foo`, `Foo12` et `Foo3`



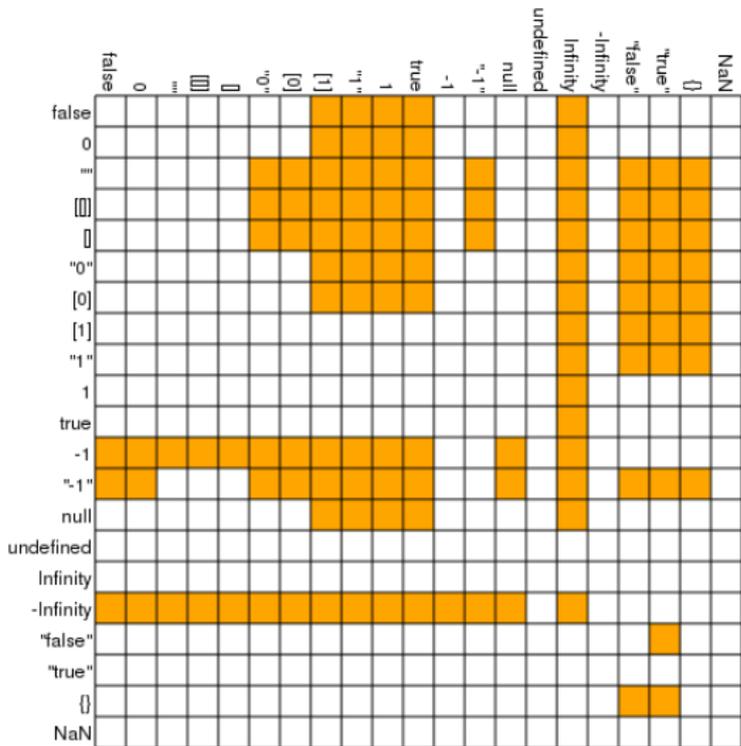
Égal ==



Plus petit ou égal <=



Plus petit <



Plus grand >



Le compilateur C cherche également à rendre service, que vaut z ?

Source (c/cast0.c)

```
{ int x=3; int y=4; float z=x/y; }
```



Le compilateur C cherche également à rendre service, que vaut z ?

Source (c/cast0.c)

```
{ int x=3; int y=4; float z=x/y; }
```

0.0



Le compilateur C cherche également à rendre service, que vaut z ?

Source (c/cast0.c)

```
{ int x=3; int y=4; float z=x/y; }
```

0.0

Source (c/cast1.c)

```
{ unsigned char x = 128; unsigned char y = 2;  
  unsigned char z = (x * y) / y; }
```



Le compilateur C cherche également à rendre service, que vaut z ?

Source (c/cast0.c)

```
{ int x=3; int y=4; float z=x/y; }
```

0.0

Source (c/cast1.c)

```
{ unsigned char x = 128; unsigned char y = 2;  
  unsigned char z = (x * y) / y; }
```

128 (ce n'est pas une optimisation du compilateur mais un *cast*)



Pour les curieux, voici le code assembleur associé à `cast1.c`

Source (c/castregister.asm)

```
unsigned char x = 128;
    movb    $-128, -19(%rbp)
unsigned char y = 2;
    movb    $2, -18(%rbp)
unsigned char z = (x * y) / y;
    movzbl  -19(%rbp), %edx
    movzbl  -18(%rbp), %eax
    imull  %edx, %eax
    movzbl  -18(%rbp), %edx
```



[JAVA] Surcharge (pond des rôles)

Le développeur peut parfois mettre son propre grain de sel

Source (java/Confuser.java)

```
class Confuser {  
  
    static void A(short i) { System.out.println("Foo"); }  
    static void A(int i) { System.out.println("Bar"); }  
  
    public static void main (String[] args) {  
        short i=0;  
        A(i);  
        A(i+i);  
        A(i+=i);  
    }  
}
```



[JAVA] Surcharge (pond des rôles)

Le développeur peut parfois mettre son propre grain de sel

Source (java/Confuser.java)

```
class Confuser {  
  
    static void A(short i) { System.out.println("Foo"); }  
    static void A(int i) { System.out.println("Bar"); }  
  
    public static void main (String[] args) {  
        short i=0;  
        A(i);  
        A(i+i);  
        A(i+=i);  
    }  
}
```

Le programme affiche `Foo`, `Bar`, `Foo`; dans la « vraie » vie ajoutez de l'héritage et des `Integer`



[RUBY] Alea jacta est !

La surcharge permet même de transformer les fondamentaux

Source (ruby/poison.rb)

```
> 3==4
=> false
> 3.eql?4
=> false
> 3.equal?4
=> false

> class Fixnum; def ==(y); true; end; end
=> nil
> 3==4
=> true
> 3.eql?4
=> true
> 3.equal?4
=> false
```

C'est aussi possible en JAVASCRIPT par exemple



[C] Complément d'information

Avant de présenter les exemples suivants, un petit rappel : combien y a-t-il de solutions pour l'équation $x = -x$ en \mathbb{C} ?

Source (c/cast2.c)

```
#include <stdio.h>

int main(void) {
    int z=0;
    if (z== -z) printf("%d==-(%d)\n",z,z);

    int r=1<<((sizeof(int)*8)-1);
    if (r== -r) printf("%d==-(%d)\n",r,r);

    return 0;
}
```

$0 == -(0)$ et $-2147483648 == -(-2147483648)$, c'est ce qui fait tout le charme du complément à 2 pour représenter les entiers signés



[C] C'est mauvais signe...

Même quand on pense avoir bien compris, il reste des surprises...

Source (c/castsigned2.c)

```
{ unsigned char a = 1; signed char b = -1;
  if (a<b) printf("%d<%d\n",a,b);
  else printf("%d>=%d\n",a,b); }

{ unsigned int a = 1; signed int b = -1;
  if (a<b) printf("%d<%d\n",a,b);
  else printf("%d>=%d\n",a,b); }
```



[C] C'est mauvais signe...

Même quand on pense avoir bien compris, il reste des surprises...

Source (c/castsigned2.c)

```
{ unsigned char a = 1; signed char b = -1;
  if (a<b) printf("%d<%d\n",a,b);
  else printf("%d>=%d\n",a,b); }

{ unsigned int a = 1; signed int b = -1;
  if (a<b) printf("%d<%d\n",a,b);
  else printf("%d>=%d\n",a,b); }
```

Avec les types `char`, on obtient `1>=-1`, alors qu'avec les types `int` on obtient `1<-1` – encore des subtilités sur les promotions



Ces mécanismes peuvent rendre certains contrôles caduques

Source (c/castbound.c)

```
#include <stdio.h>

void write(int tab[],int size,signed char ind,int val) {
    if (ind<size) tab[ind]=val;
    else printf("Fail\n");
}

int main(void) {
    size_t size=120; int tab[size];
    write(tab,size,127,42);
    write(tab,size,128,42);
    return 0;
}
```



Ces mécanismes peuvent rendre certains contrôles caduques

Source (c/castbound.c)

```
#include <stdio.h>

void write(int tab[],int size,signed char ind,int val) {
    if (ind<size) tab[ind]=val;
    else printf("Fail\n");
}

int main(void) {
    size_t size=120; int tab[size];
    write(tab,size,127,42);
    write(tab,size,128,42);
    return 0;
}
```

Première écriture refusée (**Fail**) mais seconde acceptée – le où est laissé à la sagacité de l'auditoire... Et si `size=150` ?



[C] Une vraie vulnérabilité

Si vous le lui demandez, le compilateur peut parfois vous aider à repérer ces problèmes (`-Wconversion`⁴ pour GCC)

Les plus curieux d'entre vous pourront étudier la faille CVE-2010-0740 (*Record of death vulnerability*) sur OpenSSL

Source (c/patch-CVE-2010-0740.diff)

```
- /* Send back error using their
-  * version number :-) */
- s->version=version;
+ if ((s->version & 0xFF00) == (version & 0xFF00))
+ /* Send back error using their minor version number :-) */
+ s->version = (unsigned short)version;
```

Il semble qu'une faille d'authentification sur MySQL puisse également être liée à ce type de difficultés

4. à moins que ce ne soit `-Wextra`? Ce n'est pas très clair...



Source (php/castincr.php)

```
$x="2d8"; print($x+1); print("\n");  
  
$x="2d8"; print(++$x."\n"); print(++$x."\n"); print(++$x."\n");  
  
if ("0xF9"=="249") { print("Equal\n"); }  
else { print("Different\n"); }
```



Source (php/castincr.php)

```
$x="2d8"; print($x+1); print("\n");  
  
$x="2d8"; print(++$x."\n"); print(++$x."\n"); print(++$x."\n");  
  
if ("0xF9"=="249") { print("Equal\n"); }  
else { print("Different\n"); }
```

La première ligne affiche 3 (entier)



Source (php/castincr.php)

```
$x="2d8"; print($x+1); print("\n");  
  
$x="2d8"; print(++$x."\n"); print(++$x."\n"); print(++$x."\n");  
  
if ("0xF9"=="249") { print("Equal\n"); }  
else { print("Different\n"); }
```

La première ligne affiche 3 (entier)

La seconde ligne affiche 2d9 (chaîne), 2e0 (chaîne) puis 3 (flottant)



Source (php/castincr.php)

```
$x="2d8"; print($x+1); print("\n");  
  
$x="2d8"; print(++$x."\n"); print(++$x."\n"); print(++$x."\n");  
  
if ("0xF9"=="249") { print("Equal\n"); }  
else { print("Different\n"); }
```

La première ligne affiche 3 (entier)

La seconde ligne affiche 2d9 (chaîne), 2e0 (chaîne) puis 3 (flottant)

La troisième ligne affiche Equal



Quel rapport avec la sécurité? Voici un exemple

Source (php/hash.php)

```
$s1='QNKCDZO'; $h1=md5($s1);
$s2='240610708'; $h2=md5($s2);
$s3='A169818202'; $h3=md5($s3);
$s4='aaaaaaaaaaaumdozb'; $h4=md5($s4);
$s5='badthingsrealmlavznik'; $h5=sha1($s5);

if ($h1==$h2) print("Collision\n");
if ($h2==$h3) print("Collision\n");
if ($h3==$h4) print("Collision\n");
if ($h4==$h5) print("Collision\n");
```



Quel rapport avec la sécurité? Voici un exemple

Source (php/hash.php)

```
$s1='QNKCDZO'; $h1=md5($s1);  
$s2='240610708'; $h2=md5($s2);  
$s3='A169818202'; $h3=md5($s3);  
$s4='aaaaaaaaaaaumdozb'; $h4=md5($s4);  
$s5='badthingsrealmlavznik'; $h5=sha1($s5);  
  
if ($h1==$h2) print("Collision\n");  
if ($h2==$h3) print("Collision\n");  
if ($h3==$h4) print("Collision\n");  
if ($h4==$h5) print("Collision\n");
```

`Collision` est affiché 4 fois, mais ne concluez pas trop vite que MD5 et SHA1 sont mis en cause ici



Surcharges et *casts* permettent au compilateur de tripatouiller le code jusqu'à lui trouver *un*⁵ sens

Source (js/weirdeval.js)

```
{ } + { }  
[ ] + { }  
{ } + [ ]  
( { } + { } )
```

Toutes ces expressions ont un sens différent de celui des autres (même la première et la quatrième ligne)

jscert.org donne d'autres éléments surprenants sur JAVASCRIPT

5. Article volontairement indéfini



Plan

- 1** Toi qui entres ici . . .
 - Lutte des classes
 - Mise en boîte
 - Effets spéciaux
 - Épreuves d'adresses
 - *Cast-o-rama*
 - **Rencontre du 3^e type**
 - Où tout est question d'interprétation
 - Les liaisons dangereuses
 - Syntaxe, priez pour nous



Les comportements à la marge des types sont souvent intéressants

Source (sql/partial.sql)

```
SELECT CONCAT(IF(@X<=@Y,'X<=Y','X>Y'),  
              ' and ',  
              IF(@X>=@Y,'X>=Y','X<Y')) AS Test;
```

Avec SET @X=1; SET @Y=2; on obtient X<=Y and X<Y



Les comportements à la marge des types sont souvent intéressants

Source (sql/partial.sql)

```
SELECT CONCAT(IF(@X<=@Y,'X<=Y','X>Y'),  
              ' and ',  
              IF(@X>=@Y,'X>=Y','X<Y')) AS Test;
```

Avec `SET @X=1; SET @Y=2;` on obtient `X<=Y and X<Y`

Avec `SET @X=NULL` par contre on obtient `X>Y and X<Y` (le même type d'observations peut être fait avec les flottants et `NaN`)



[OCAML] Certains sont plus égaux que d'autres

En OCAML, x et y étant des valeurs, combien de valeurs peut prendre l'expression booléenne $x=y$?



[OCAML] Certains sont plus égaux que d'autres

En OCAML, x et y étant des valeurs, combien de valeurs peut prendre l'expression booléenne $x=y$?

Source (ocaml/bool4.ml)

```
type tree= Leaf | Node of tree*tree;;

let zero = Leaf;;
let one = Node(Leaf,Leaf);;
let rec many = Node(Leaf,many);;
let rec more = Node(more,Leaf);;
```

`zero=zero` donne `true`, `zero=one` donne `false`, `many=many` boucle et `more=more` provoque une erreur – donc 4 comportements



[Shell] Interdiction d'interdire

Pas convaincu par la remarque précédente ? Et pourtant...

Source (shell/login.sh)

```
#!/bin/bash
PIN=1234
echo -n "Please type your PIN code (4 digits): "
read -s PIN_TYPED; echo

if [ "$PIN" -ne "$PIN_TYPED" ]; then
    echo "Invalid PIN code."; exit 1
else
    echo "Authentication OK"; exit 0
fi
```



[Shell] Interdiction d'interdire

Pas convaincu par la remarque précédente ? Et pourtant...

Source (shell/login.sh)

```
#!/bin/bash
PIN=1234
echo -n "Please type your PIN code (4 digits): "
read -s PIN_TYPED; echo

if [ "$PIN" -ne "$PIN_TYPED" ]; then
    echo "Invalid PIN code."; exit 1
else
    echo "Authentication OK"; exit 0
fi
```

Un mauvais code PIN sera rejeté ; par contre, si l'utilisateur saisit des caractères non numériques, l'accès lui sera accordé



Focus sur la vulnérabilité *Goto Fail* de GNUTLS en mars 2014 (lwn.net)

But this bug is arguably much worse than APPLE's, as it has allowed crafted certificates to evade validation check for all versions of GNUTLS ever released since that project got started in late 2000.[...]

*The `check_if_ca` function is supposed to return true (any non-zero value in C) or false (zero) depending on whether the issuer of the certificate is a certificate authority (CA). A true return should mean that the certificate passed muster and can be used further, but the bug meant that **error returns were misinterpreted as certificate validations.***



Petit rappel historique sur une vulnérabilité OPENSSL remontant à 2008 (CVE-2008-5077)

Le patch correctif remplace `if (!i)` par `if (i<=0)`, la valeur `i` en question étant le retour d'une fonction vérifiant un certificat, qui était interprétée un peu vite comme un booléen pur **sans prendre en compte les autres valeurs correspondant à un code d'erreur**

Oui, c'est *exactement* le même problème que le *Goto Fail* de GNUTLS en 2014, sur exactement le même type de fonction sur exactement le même type de logiciel critique, donc de deux choses l'une

- ▶ Soit on continue de critiquer les développeurs qui n'apprennent pas
- ▶ Soit on considère que peut-être les outils et les langages ne sont pas adaptés



Comportements atypiques

Les types statiques constituent une information purement logique qui n'a aucune existence concrète dans l'implémentation

Il faut donc éviter des raisonnements étreiqués excluant des situations « mal typées » mais néanmoins possibles

- ▶ Désérialisation de valeurs incohérentes en OCAML ou PYTHON
- ▶ Attaque *Wrap & Decipher* sur l'API PKCS#11
- ▶ ...



- 1 Toi qui entres ici...
 - Lutte des classes
 - Mise en boîte
 - Effets spéciaux
 - Épreuves d'adresses
 - *Cast-o-rama*
 - Rencontre du 3^e type
 - Où tout est question d'interprétation
 - Les liaisons dangereuses
 - Syntaxe, priez pour nous



On peut en PHP faire appel à un interpréteur SQL

Source (php/injectionsql.php)

```
$dbc=mysqli_connect(HST,LOG,PWD,"School");  
$cmd="SELECT * FROM Students WHERE id='".$val."'";  
$dbr=mysqli_query($dbc,$cmd);
```



On peut en PHP faire appel à un interpréteur SQL

Source (php/injectionsql.php)

```
$dbc=mysqli_connect(HST,LOG,PWD,"School");  
$cmd="SELECT * FROM Students WHERE id='".$val."'";  
$dbr=mysqli_query($dbc,$cmd);
```

Bien entendu, si `$val="Bobby'; DROP TABLE Students; //"`...

Cette notion d'injection est très générique, dans le domaine des applications *web* (XSS, CSRF...) comme ailleurs



L'injection résulte donc de l'utilisation d'un interpréteur, en général celui d'un autre langage

Source (ocaml/syscommand.ml)

```
let printfile filename =  
  Sys.command("cat "^filename);;
```

6. Les auteurs déclinent toute responsabilité en cas d'essais



L'injection résulte donc de l'utilisation d'un interpréteur, en général celui d'un autre langage

Source (ocaml/syscommand.ml)

```
let printfile filename =  
  Sys.command("cat "^filename);;
```

printfile "texput.log" aura le résultat escompté
printfile "--version ; cd / ; rm -ri ." sans doute pas⁶

6. Les auteurs déclinent toute responsabilité en cas d'essais



[RUBY/Shell] Ceci n'est pas un pipe

En RUBY, `Kernel.open` et `File.open` permettent d'ouvrir un fichier et ont presque le même comportement. . . Le premier (celui invoqué par `open`) permet en fait de fichier de récupérer la sortie d'une commande *Shell*

Source (ruby/injectionshell.rb)

```
> open ("|ls").each { |x| p x }
"beginend.rb\n"
"beginend.rb~\n"
...
```

Sur quel critère ? Le fait que le nom de fichier commence par le caractère |



[PHP] Moins d'évaluation pour plus de sécurité

Certains langages interprétés proposent un évaluateur interne

Source (php/injectioneval.php)

```
$cmd1="echo 'Hello ".$val."\n';";  
  
eval($cmd1);
```

Avec `$val` valant `''; die('eval killed me'); //` par exemple on dévie du comportement imaginé

C'est bien sur dangereux, mais surtout impossible à analyser



D'autres constructions, sans être des évaluateurs, sont également inquiétantes (ne parlons même pas de lisibilité ou de traçabilité)

Source (php/injectionvar.php)

```
function hello() { echo "Hello world<br />"; }  
function goodbye() { echo "Good bye<br />"; }  
  
$x="hello"; $x();  
  
$y="x"; $$y="goodbye"; $x();
```

Hello world

Good bye

Mais heureusement « personne ne fait ça »⁷

7. Sauf pas mal de *frameworks* pour le développement *web*



Une fois le concept d'injection bien compris, on en arrive à se poser des questions curieuses par exemple sur le *Shell*...

On peut utiliser `*` en paramètre dans une ligne de commande ; *a priori* c'est simple, pourtant il peut y avoir des questions assez subtiles, par exemple que se passe-t-il s'il existe un fichier nommé `"*`, `"-o"`, `">rights.acl"` ou encore `"; rm *` ?



Une fois le concept d'injection bien compris, on en arrive à se poser des questions curieuses par exemple sur le *Shell*...

On peut utiliser `*` en paramètre dans une ligne de commande ; *a priori* c'est simple, pourtant il peut y avoir des questions assez subtiles, par exemple que se passe-t-il s'il existe un fichier nommé `"*`, `"-o"`, `">rights.acl"` ou encore `"; rm *` ?

Rien... si ce n'est qu'un fichier dont le nom commence par `"-` sera généralement interprété *par la commande appelée* comme une option



Une fois le concept d'injection bien compris, on en arrive à se poser des questions curieuses par exemple sur le *Shell*...

On peut utiliser `*` en paramètre dans une ligne de commande ; *a priori* c'est simple, pourtant il peut y avoir des questions assez subtiles, par exemple que se passe-t-il s'il existe un fichier nommé `"*`, `"-"`, `">rights.acl"` ou encore `;" rm *` ?

Rien... si ce n'est qu'un fichier dont le nom commence par `"-` sera généralement interprété *par la commande appelée* comme une option

Un autre détail : si vous exécutez `cat foo*` dans un répertoire ne contenant aucun fichier de la forme `foo*`, vous savez ce que le *Shell* passe en paramètre à la commande `cat` ?



1 Toi qui entres ici...

- Lutte des classes
- Mise en boîte
- Effets spéciaux
- Épreuves d'adresses
- *Cast-o-rama*
- Rencontre du 3^e type
- Où tout est question d'interprétation
- **Les liaisons dangereuses**
- Syntaxe, priez pour nous



PYTHON offre une construction syntaxique proche du `map` classique sur les listes, la définition de listes en compréhension

Source (python/listcomp.py)

```
>>> l = [s+1 for s in [1,2,3]]
>>> l
[2, 3, 4]
```

Que se passe-t-il si ensuite on tape `s` à l'invite ?



PYTHON offre une construction syntaxique proche du `map` classique sur les listes, la définition de listes en compréhension

Source (python/listcomp.py)

```
>>> l = [s+1 for s in [1,2,3]]
>>> l
[2, 3, 4]
```

Que se passe-t-il si ensuite on tape `s` à l'invite ?

à moins d'utiliser la dernière version de Python 3, `s` vaut 3, alors que la variable `s` devrait être locale (liée)



Un autre comportement intrigant

Source (python/localvar3.py)

```
source = [1,2,3,4]
dest = [0] * 4

def copy1 ():
    dest = source

def copy2 ():
    for i in range(4):
        dest[i]=source[i]
```

Initialement `dest` vaut `[0,0,0,0]`, après l'appel de `copy1()` il vaut toujours `[0,0,0,0]`, et après l'appel de `copy2()` il vaut `[1,2,3,4]`



En fait scripts et localité ne semblent pas faire bon ménage

Source (php/link.php)

```
$var = "var";  
$tab = array("foo ", "bar ", "blah ");  
  
echo "Tab="; echo $tab; echo " ; ";  
echo "Loop="; { foreach ($tab as $var) { echo $var; } }  
echo " ; ";  
  
echo "Var="; echo $var;
```



En fait scripts et localité ne semblent pas faire bon ménage

Source (php/link.php)

```
$var = "var";  
$tab = array("foo ", "bar ", "blah ");  
  
echo "Tab="; echo $tab; echo " ; ";  
echo "Loop="; { foreach ($tab as $var) { echo $var; } }  
echo " ; ";  
  
echo "Var="; echo $var;
```

On obtient `Tab=Array ; Loop=foo bar blah ; Var=blah`, la variable `var` est écrasée et survit à la boucle ! Les plus audacieux pourront tester `foreach ($tab as $tab)...`



Plan

- 1 **Toi qui entres ici...**
 - Lutte des classes
 - Mise en boîte
 - Effets spéciaux
 - Épreuves d'adresses
 - *Cast-o-rama*
 - Rencontre du 3^e type
 - Où tout est question d'interprétation
 - Les liaisons dangereuses
 - **Syntaxe, priez pour nous**



[C] Compromission sans condition

Une modification du noyau LINUX⁸

Source (c/kernel.diff)

```
+ if ((options==( __WCLONE | __WALL )) && (current->uid=0))  
+  retval = -EINVAL;
```

8. Cf. lwn.net/Articles/57135/



[C] Compromission sans condition

Une modification du noyau LINUX⁸

Source (c/kernel.diff)

```
+ if ((options==( __WCLONE|__WALL)) && (current->uid=0))  
+  retval = -EINVAL;
```

Piégeage pur et simple : lorsque la condition sur `options` est vraie, `current->uid` devient 0 (*i.e.* le process passe `root`)

L'attaquant joue sur la confusion entre = et ==, mais aussi le fait que l'affectation renvoie une valeur, que le typage ne distingue pas un booléen d'un entier, que le et booléen est paresseux, *etc.*

8. Cf. lwn.net/Articles/57135/



Petite caractéristique intrigante des commentaires OCAML

Source (ocaml/comments.ml)

```
(* blah blah " blah blah *)  
let x=true;;  
  
(* PREVIOUS VERSION -----  
(* blah blah " blah blah *)  
let x=false;;  
(* blah blah " blah blah *)  
-----*)  
  
(* blah blah " blah blah *)
```



Petite caractéristique intrigante des commentaires OCAML

Source (ocaml/comments.ml)

```
(* blah blah " blah blah *)  
let x=true;;  
  
(* PREVIOUS VERSION -----  
(* blah blah " blah blah *)  
let x=false;;  
(* blah blah " blah blah *)  
-----*)  
  
(* blah blah " blah blah *)
```

Il est possible d'ouvrir une chaîne de caractères dans un commentaire OCAML, ce qui peut induire en erreur un relecteur, surtout si la coloration syntaxique n'est pas conforme



[C] Long discours ou petit dessin ?

Les commentaires visuels ne sont pas toujours les plus utiles

Source (c/comments2.c)

```
#include <stdio.h>

int main(void) {

// !\ DO NOT REMOVE COMMENTS IN NEXT BLOCK !\
/*****
    const char status []="Safe";
// !\ SET TO SAFE ONLY FOR TESTS !\
*****/

// !\ NEXT LINE REALLY IMPORTANT !\
    const char status []="Unsafe";
    printf("Status: %s\n",status);
}
```

Status: Safe (à moins qu'il n'y ait des espaces ici ou là...)



[C] Trop de commentaires tuent le commentaire

Les commentaires sont parfois vraiment délicats à traiter

Source (c/comments.c)

```
#include <stdio.h>

int foo() {
    int a=4; int b=2;
    return a /*
                /*/ b
;
}

int main(void) {
    printf("%d\n",foo()); return 0;
}
```

Ce code, compilé et exécuté, affiche 4; mais si on compile en mode C89 (option `-std=c89` de GCC) on obtient 2



Certains compilateurs sont compatibles avec l'encodage UTF-8

Source (java/Preprocess.java)

```
public class Preprocess {  
    public static void main (String[] args) {  
        if (false==true)  
        { //\u000a\u0007d\u0007b  
            System.out.println("Bad things happen!");  
        }  
    }  
}
```

Bad thing happens : le code source est donc *a priori* préprocessé préalablement à la compilation



La norme ANSI pour le C permet l'utilisation de claviers auxquels il manque des caractères utiles

La norme définit donc des *trigraphes*

- ▶ ??= devient #
- ▶ ??/ devient \
- ▶ ??' devient ~
- ▶ ??(devient [
- ▶ ??< devient {
- ▶ ??! devient |
- ▶ ??) devient]
- ▶ ??> devient }
- ▶ ??- devient ~

Donc si vous voyez un commentaire de la forme `// Blah ??/` vous saurez à quoi (ne pas) vous en tenir...



[RUBY] Un saut dans l'espace

Certains choix de syntaxe sont incompréhensibles, et ne peuvent que mener à des erreurs lors du développement

Source (ruby/break.rb)

```
def test1 (x,y)
  x +
  y
end

def test2 (x,y)
  x
  + y
end
```

test1 (1,2) retourne 3, test2(1,2) retourne 2



Un autre choix de syntaxe bizarre, toujours en RUBY

Source (ruby/parentheses.rb)

```
> def test(x); x*2; end
=> nil

> test 1
=> 2
> test(1)
=> 2
> test(1)+1
=> 3
> test (1)+1
=> 4
```



[C] Epic Apple's Goto Fail

Encore un bug dans une bibliothèque cryptographique révélé en 2014

Source (c/gotofail.c)

```
/* Extract from Apple's sslKeyExchange.c */
if ((err=SSLHashSHA1.update(&hashCtx,&serverRandom))!=0)
    goto fail;
if ((err=SSLHashSHA1.update(&hashCtx,&signedParams))!=0)
    goto fail;
if ((err=SSLHashSHA1.final(&hashCtx,&hashOut))!=0)
    goto fail;
```

La syntaxe n'aide pas, mais le compilateur ne semble pas non plus se préoccuper de signaler du code manifestement mort...



Plan

- 1 Toi qui entres ici. . .
- 2 Au-delà des illustrations
- 3 Quelques éléments de conclusion



Extrait de la spécification officielle du langage JAVA relative à la méthode `clone` de la classe `Object`

*The **general intent** is that, for any object x , the expression :*

`x.clone() != x` will be true, and that the expression :

*`x.clone().getClass() == x.getClass()` will be true, but these are **not absolute requirements**. While it is **typically** the case that :*

*`x.clone().equals(x)` will be true, this is **not** an absolute requirement.*

La spécification des opérations de sérialisation (`writeObject` et `readObject`) est aussi assez intrigante



RUBY intègre des mécanismes de sécurité. . .

The first [part] is a mechanism for distinguishing safe data from untrusted, or tainted, data. The second [part] is a technique for restricted execution, which allows you to “lock down” the Ruby environment and prevents the Ruby interpreter from performing potentially dangerous operations on tainted data.

Lesquels exactement et avec quelle robustesse reste à déterminer !

Furthermore, keep in mind that Ruby’s security model has not received the kind of careful and prolonged scrutiny that Java’s security architecture has.



[C] Pointless pointer operations

Encore un extrait de “*The C programming language (Second edition)*”

The meaning of “adding 1 to a pointer,” and by extension, all pointer arithmetic, is that $pa+1$ points to the next object, and $pa+i$ points to the i -th object beyond pa .

En d'autres termes, l'effet de `p++` dépend du type pointé, et plus exactement de la taille de sa représentation mémoire – qui peut être obtenue notamment par l'utilisation de l'opérateur `sizeof` ; c'est relativement intuitif



[C] Pointless pointer operations

Encore un extrait de “*The C programming language (Second edition)*”

The meaning of “adding 1 to a pointer,” and by extension, all pointer arithmetic, is that $pa+1$ points to the next object, and $pa+i$ points to the i -th object beyond pa .

En d'autres termes, l'effet de `p++` dépend du type pointé, et plus exactement de la taille de sa représentation mémoire – qui peut être obtenue notamment par l'utilisation de l'opérateur `sizeof` ; c'est relativement intuitif

Ceci dit que se passe-t-il exactement si `p` est un pointeur de fonction en architecture CISC ? Cette question est dénuée de sens. . . mais le code correspondant est compilable et exécutable



[C] L'auberge espagnole

Un extrait de “*The C programming language (Second edition)*” de B. W. Kernighan & D. M. Ritchie

The direction of truncation for / and the sign of the result for % are machine-dependent for negative operands, as is the action taken on overflow or underflow.

La question est de savoir comment **tester** la conformité d'un compilateur à cette spécification non-déterministe. . . Pensez-y



[C] L'auberge espagnole

Un extrait de “*The C programming language (Second edition)*” de B. W. Kernighan & D. M. Ritchie

The direction of truncation for / and the sign of the result for % are machine-dependent for negative operands, as is the action taken on overflow or underflow.

La question est de savoir comment **tester** la conformité d'un compilateur à cette spécification non-déterministe. . . Pensez-y

Votre test rejeterait-il un compilateur changeant l'arrondi à **chaque appel**, ce qui permettrait d'avoir $1/-2==1/-2$ évalué à faux ? C'est une instanciation de ce qu'on appelle le *Paradoxe du raffinement*, résolu avec le standard C99



[JAVA] Questions d'exécution capitales

JAVA est un langage qui se compile en *bytecode* vérifié et interprété par une JVM ; cela peut susciter quelques questions :

- ▶ Peut-on écrire en *bytecode* plus de choses qu'en JAVA ? Les vérifications sont-elles bien pensées au niveau *bytecode* ?
- ▶ Peut-on empêcher l'exécution d'un *bytecode* en restreignant les droits au niveau du système de fichiers (`chmod a-x`) ?
- ▶ Peut-on empêcher l'exécution d'un *bytecode* présent en mémoire en marquant sa page comme non exécutable ?
- ▶ La JVM est-elle compatible avec les mécanismes de prévention d'exécution de certaines pages mémoire ?
- ▶ Quelle relation entre privilèges du *bytecode* et de la JVM ?

Bref quelle sont les conséquences sur l'efficacité ou la possibilité de mettre en œuvre des mécanismes de sécurité système ?



OCAML met en œuvre un GC qui gère la mémoire ; supposons que nous voulions implémenter très proprement une bibliothèque cryptographique manipulant des clés secrètes et/ou privées

- ▶ Comment interdire les copies (compactage ou *swap*) ?
- ▶ Comment minimiser la durée de présence d'une clé en mémoire ?
- ▶ Comment effacer une clé par surcharge ?

Au passage, notons qu'un mécanisme non fonctionnel⁹ tel que la surcharge peut aussi être victime d'optimisations de compilation, de mécanismes de cache, de technologies telles que celle des mémoires *flash* ou de tout autre mécanisme d'optimisation du même type

9. C'est à dire sans effet visible sur les résultats de l'exécution



[JAVA] Le facteur humain (sonne toujours 3 fois)

Cf. thedailywtf.com/Articles/Java-Destruction.aspx

Source (java/Destruction.java)

```
public class Destruction {  
    public static void delete (Object object) {  
        object = null;  
    }  
}
```

Plus de 160 commentaires en réponse, dont

- ▶ *Obviously the problem is that he forgot to call `System.gc()`*
- ▶ *It allows the object to be garbage collected... It is still a [problem] because a one liner should be done by the caller*
- ▶ *You know nulling objects to "help" the garbage collector is usually considered bad practice, right ?*
- ▶ *Maybe the coder was used to VB, where parameters are sent ByRef by default ?*



[Web] Question de philosophie. . .

Sur stackoverflow.com/questions/4456438/how_...

How can I pass the string "Null" through WSDL (SOAP) from ACTIONSCRIPT 3 to a COLDFUSION web service without receiving a "missing parameter error" ? We have an employee whose last name is Null. He kills our employees lookup application when his last name is used as the search term. . .

C'est sans doute une plaisanterie. . . Mais elle fait réfléchir



Plan

- 1 Toi qui entres ici. . .
- 2 Au-delà des illustrations
- 3 Quelques éléments de conclusion



À propos du développement

À quoi devrait être attentif un développeur ?

- ▶ Les langages ne sont pas vos amis : coder sécurisé, c'est comme jongler avec des tronçonneuses
- ▶ Sélectionner les « bons » langages et *frameworks*
 - ▶ Faire de la cryptographie en JAVASCRIPT est... délicat
 - ▶ À défaut utiliser les bons outils et les bonnes options
- ▶ Maîtriser chaque langage utilisé
 - ▶ Faux amis, mots clés communs avec des sens différents
 - ▶ Robustesse des mécanismes proposés
 - ▶ Ne pas abuser des gadgets, ne pas laisser l'ordinateur deviner
 - ▶ Limiter le recours aux traits les plus dynamiques
- ▶ Connaître les fondamentaux¹⁰
- ▶ Ne pas forcer son talent
- ▶ Se méfier des codes tiers

10. Sémantique des langages, compilation, OS, architecture des ordinateurs...



À propos des langages

Comment aider à l'amélioration de la sécurité ou de l'assurance ?

- ▶ La spécification d'un langage est idéalement complète, déterministe et non ambiguë (voire formalisée)
- ▶ *Simple is beautiful*
 - ▶ Ne conserver que ce qui est nécessaire
 - ▶ Éviter ce qui est complexe ou dénué de sens
 - ▶ Ne pas contrarier l'intuition ou la logique élémentaire
- ▶ Sans maîtrise, la puissance n'est rien
 - ▶ Faciliter la lisibilité et la traçabilité : un mot clé pour un concept, des notations cohérentes, *etc.*
 - ▶ Ne pas confondre aide au développeur avec laxisme ou devinettes
 - ▶ Introspection, évaluation, traits dynamiques rendent toute forme d'analyse délicate voire impossible



À propos des outils

Quels outils (ou options) pour la sécurité et l'assurance ?

- ▶ Ce qui n'est pas spécifié pour le langage devrait être interdit par les outils – ou au moins signalé
- ▶ Implémenter les vérifications possibles, et les faire au plus tôt
- ▶ Minimiser les manipulations silencieuses
- ▶ Savoir aller au-delà du fonctionnel
 - ▶ Le raisonnement de sécurité nécessite de penser au-delà des interfaces d'une boîte noire
 - ▶ Certaines optimisations sont inappropriées en sécurité
- ▶ Étendre le domaine des invariants de compilation¹¹
 - ▶ Modèle mémoire reflétant l'encapsulation
 - ▶ Préserver le flot d'exécution même en présence de fautes
- ▶ Disposer d'outils maîtrisés voire de confiance

11. Cela peut aussi concerner les architectures...



Remerciements

Les exemples de cette présentation sont fournis ou inspirés par :

- ▶ Les laboratoires de l'ANSSI
- ▶ Les participants à l'étude JAVASEC
- ▶ Les participants à l'étude LAFOSEC
- ▶ Différents sites et blogs, notamment :
 - ▶ www.thedailywtf.com, www.xkcd.com
 - ▶ le site de la société MLSTATE
 - ▶ *Sami Koivu (Slightly Random Broken Thoughts)*
 - ▶ *Jeff Atwood (Coding Horror)*
 - ▶ *Software Engineering Not At School*
 - ▶ *Functional Orbitz*
 - ▶ *Rob Kendrick (Some dark corners of C)*

Sans oublier, bien entendu, l'aimable collaboration des concepteurs des langages et des outils ;-)



Outils et langages utilisés

- ▶ **C** : gcc (Ubuntu/Linaro 4.6.3-1ubuntu5) 4.6.3
- ▶ **ERLANG** : Erlang R14B04 (erts-5.8.5)
- ▶ **JAVA** : Eclipse Java Compiler 0.972_R35x, 3.5.1 release
- ▶ **JAVASCRIPT** : Mozilla Firefox 16.0.2 for Ubuntu canonical - 1.0
- ▶ **SQL** : mysql Ver 14.14 Distrib 5.5.28, for debian-linux-gnu (i686)
- ▶ **OCAML** : The Objective Caml compiler, version 3.12.1
- ▶ **PHP** : Server version: Apache/2.2.22 (Ubuntu)
- ▶ **PYTHON 3**
- ▶ *Shell* : GNU bash, version 4.2.24(1)-release (i686-pc-linux-gnu)



4 Citations

Come, let us go down and confuse their language so they will not understand each other.

Babel, Genesis 11 :7

If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.

Gerald M. Weinberg

Software and cathedrals are very much the same – first we build them, then we pray.

Sam Redwine

All animals are equal, but some animals are more equal than others.

Animal Farm, George Orwell

Everyone knows that debugging is twice as hard as writing programs in the first place. So if you're as clever as you can be when you write it, how will you ever debug it.

Brian Kernighan

There are two ways of constructing a software design. One way is to make it so simple that there are obviously no deficiencies. And the other way is to make it so complicated that there are no obvious deficiencies.

C.A.R Hoare

Don't get suckered in by comments, they can be terribly misleading.

Dave Storer

Beware of bugs in the above code ; I have only proved it correct, not tried it.

Donald Knuth